# FortiOS Carrier - Administration Guide

Version 6.2.15

**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO GUIDE**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**FORTINET TRAINING INSTITUTE**
https://training.fortinet.com

**FORTIGUARD CENTER**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

June 8, 2023
FortiOS Carrier 6.2.15 Administration Guide
01-6215-126436-20230608

# TABLE OF CONTENTS

# Change log

| Date | Change description |
|---|---|
| June 8, 2023 | FortiOS 6.2.15 document release. |
| April 12, 2023 | FortiOS 6.2.14 document release. |
| February 23, 2023 | FortiOS 6.2.13 document release. The FortiGate-2600F and 2601F can be licensed for FortiOS Carrier, see FortiOS Carrier licensing on page 8. |
| November 3, 2022 | FortiOS 6.2.12 document release. |

# FortiOS Carrier

You can use FortiOS Carrier to apply filtering and content checking to GPRS Tunneling Protocol (GTP) traffic as it passes through 2G, 3G, 4G, and 5G carrier networks. FortiOS Carrier can also act as an SCTP firewall and FortiOS Carrier can filter Multimedia messaging service (MMS) traffic.

## FortiOS Carrier licensing

FortiOS Carrier 6.2.15 runs on the 3000, 4000, and 5000 series FortiGate platforms and on the FortiGate-2600F and 2601F.

FortiOS Carrier 6.2.15 also runs on VM08/VM08-v, VM16/VM16-v, VM32/VM32-v, and VMUL/VMUL-v series. FortiOS Carrier is not supported for the VM S-Series.

To run FortiOS Carrier you must purchase a FortiOS Carrier license from Fortinet. Once you have a license key, you should upgrade your FortiGate device or VM to the FortiOS software version that you want to be running and then use the following command from the FortiOS CLI to license your product for FortiOS Carrier:

```
execute forticarrier-license <license-key>
```

The FortiGate restarts and is set to the FortiOS Carrier factory default configuration. You can configure and operate a FortiGate running FortiOS Carrier just like a normal FortiGate. For example, you can upgrade the firmware by downloading and installing a new FortiOS firmware version or through FortiGuard. You do not have to re-license your FortiGate for FortiOS Carrier after installing new FortiOS firmware.

## FortiOS Carrier features

FortiOS Carrier supports all standard FortiOS features including SCTP firewalling. FortiOS Carrier adds the following additional features, specific to FortiOS Carrier:

- Protection for GTPv0, GTPv1, and GTPv2 traffic in 2G, 3G, 4G, and 5G carrier networks, FortiOS carrier can be installed in a wide variety of locations in any GTP network to apply various types of GTP protection depending on traffic and security needs.including:
  - GTP tunnel limiting.
  - APN traffic filtering.
  - Message filtering.
  - Message rate limiting.
  - Various other methods of filtering GTP traffic based on content, addresses, technology, and so on.
  - GTP protocol anomaly detection.
  - Information element (IE) validation and removal.
  - Encapsulated IP traffic filtering.
  - Anti-overbilling protection.
- MMS filtering to apply various filtering techniques to protect and secure MMS traffic on your network.

# FortiOS Carrier GTP protection

GTP is a protocol that encapsulates general packet radio service (GPRS) traffic to transmit the GPRS traffic over TCP/IP networks. GTP is compatible with GSM (2G), UMTS (3G), LTE (4G), and 5G networks. GTP can transport GPRS traffic over the internet and over private TCP/IP and IMS networks and is compatible with IPv4 and IPv6.

FortiOS Carrier supports GTPv0, GTPv1, and GTPv2 for 2G, 3G, 4G, and 5G networks by allowing you to create GTP profiles. These profiles allow you to apply multiple types of filtering and content checking to GTP traffic passing through FortiOS Carrier.

Once you have created GTP profiles, you can create firewall policies that accept the GTP traffic that you want to apply the GTP profile to.

To configure GTP profiles from the CLI, use the command `config firewall gtp`.

To configure GTP profiles from the GUI, go to **Security Profiles > GTP Profiles**.

Creating GTP profiles is described in Configuring GTP profiles on page 23.

## FortiOS Carrier in your GTP network

FortiOS Carrier needs to have access to all traffic entering and exiting the carrier network for scanning, filtering, and logging purposes. This promotes one of two configurations — hub and spoke, or bookend.

A hub and spoke configuration with FortiOS Carrier at the hub and the other GPRS devices on the spokes is possible for smaller networks where a lower bandwidth allows you to divide one unit into multiple virtual domains to fill multiple roles on the carrier network. It can be difficult with a single FortiOS Carrier as the hub to ensure all possible entry points to the carrier network are properly protected from potential attacks such as relayed network attacks.

A bookend configuration uses two FortiOS Carrier devices to protect the carrier network between them with high bandwidth traffic. One FortiOS Carrier handles traffic from mobile stations, SGSNs, and foreign carriers. The other handles GGSN and data network traffic. Together they ensure the network is secure.

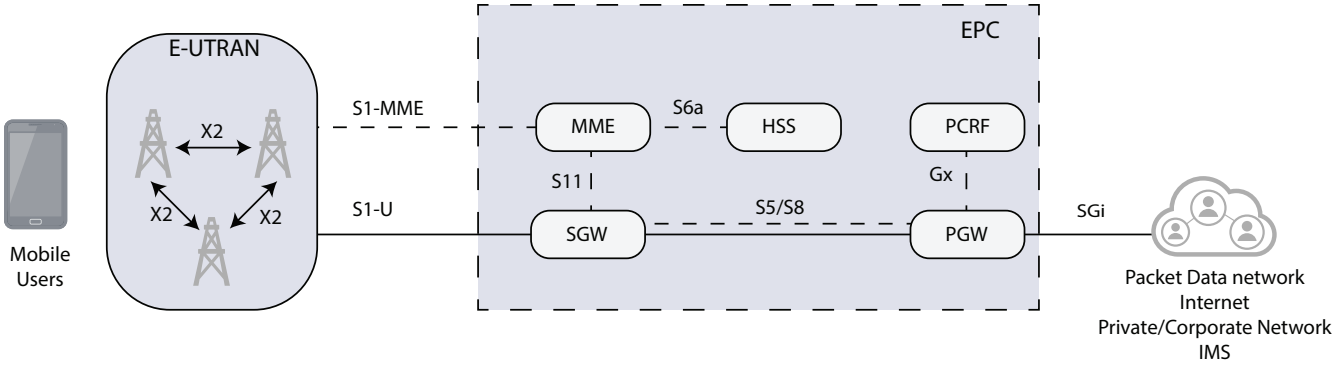
FortiOS Carrier can access all traffic on the network. It can also verify traffic between devices, and verify that the proper GPRS interface is being used. For example there is no reason for a Gn interface to be used to communicate with a mobile station — the mobile station will not know what to do with the data — so that traffic is blocked.

## GTPv2 - evolving packet core architecture

GTPv2, defined in 3GPP TS 29.274, is dramatically different from GTPv1. For example, the following diagram shows how the Evolved Packet Core (EPC) manages user data flow between mobile users (UE) and the data network. The EPC includes the following components:

- Mobility Management Entity (MME) that accepts mobile user data and performs tasks with it such as Bearer Control
- Home Subscriber Server (HSS) that performs tasks such as authentication and services automation
- Serving Gateway (SGW) that performs tasks such as Mobility Anchoring

- Packet data network Gateway (PGW) that performs tasks such as UE IP address allocation
- Policy and Charging Rules Function (PCRF) that performs tasks such as controlling QoS and throughput




FortiOS Carrier can be installed in any of the GTP data streams in your network, depending on the type of protection that you need. For overall protection you can install FortiOS Carrier between the mobile users and the EPC. If you are concerned about protecting the EPC from the internet or about protecting packet data networks, you can install FortiOS Carrier between the EPC and any TCP/IP networks that the EPC connects to.

# FortiOS Carrier and GTPv1 networks

A sample GTP network consists of the end handset sender, the sender's mobile station, the carrier's network including the SGSN and GGSN, the receiver's mobile station, and the receiver handset.

When a handset moves from one mobile station and SGSN to another, the handset's connection to the Internet is preserved because the tunnel the handset has to the Internet using GTP tracks the user's location and information. For example, the handset could move from one cell to another, or between countries.

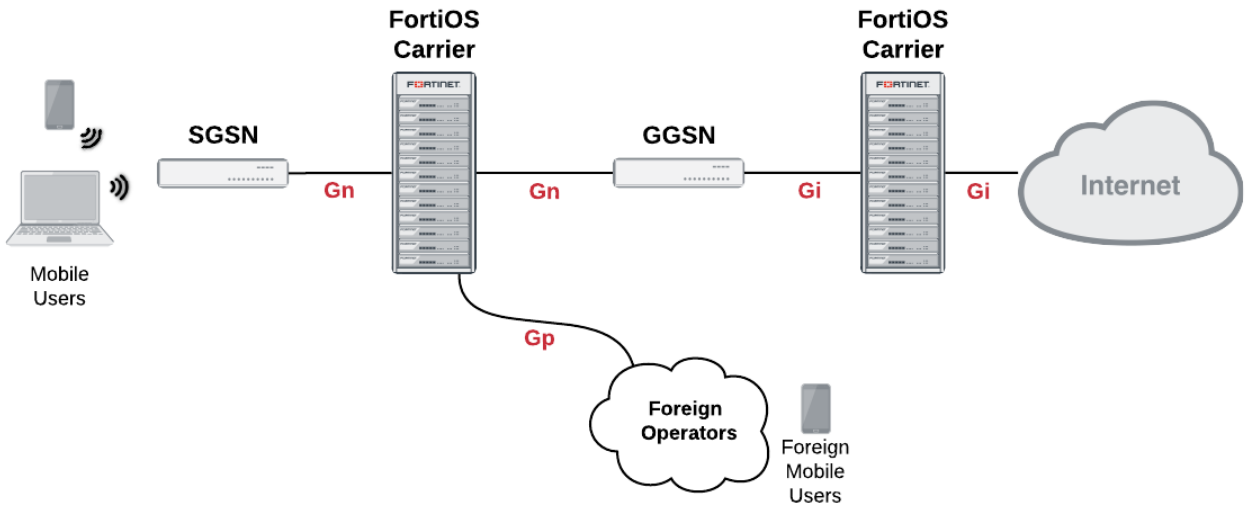
The parts of a GPRS network can be separated into the following groups according to the roles of the devices:

- Radio access to the GPRS network is accomplished by mobile phones and mobile stations (MS).
- Transport the GPRS packets across the GPRS network is accomplished by SGSNs and GGSNs, both local and remote, by delivering packets to the external services.
- Billing and records are handled by CDF, CFR, HLR, and VLR devices.

GPRS networks also rely on access points and PDP contexts as central parts of the communication structure. These are not actual devices, but they are still critical.

These devices, their roles, neighboring devices, the interfaces and protocols they use are outlined in the following table.

**Carrier network showing the interfaces used (GTPv1)**




**Devices on a GTPv1 network**

| Device role | Neighboring Devices | Interfaces used | Protocols used |
|---|---|---|---|
| Mobile Users | Mobile Stations (MS) | Radio Access Technology (RAT) | |
| Mobile Stations (MS) | Mobile Users, SGSN | Gb | IP, Frame Relay |
| SGSN (local) | MS, SGSN (local or remote), GGSN (local and remote), CDR, CFR, HLR, VLR | Ga, Gb, Gn, Gp, Gz | IP, Frame Relay, GTP, GTP' |
| SGSN (remote) | SGSN (local) | Gn | GTP |
| GGSN (local) | SGSN (local or remote), GGSN (local and remote), CDR, CFR, HLR, VLR | Ga, Gi, Gn, Gp, Gz | IP, GTP, GTP' |
| GGSN (remote) | SGSN (local), WAP gateway, Internet, other external services | Gi, Gp | IP, GTPv1 |
| CDR, CFR | SGSN (local), GGSN (local) | Ga, Gz | GTP' |
| HLR, VLR | SGSN (local), GGSN (local) | Ga, Gz | GTP' |

# PDP context

The packet data protocol (PDP) context is a connection between a mobile station and the end address that goes through the SGSN and GGSN. It includes identifying information about the mobile customer used by each server or device to

properly forward the call data to the next hop in the carrier network, typically using a GTP tunnel between the SGSN and GGSN.

When a mobile customer has an active voice or data connection open, both the SGSN and GGSN have the PDP context information for that customer and session.

When a mobile phone attempts to communicate with an address on an external packet network, either an IP or X.25 address, the mobile station that phone is connected to opens a PDP context through the SGSN and GGSN to the end address. Before any traffic is sent, the PDP context must first be activated.

The information included in the PDP context includes the customer's IP address, the IMSI number of the mobile handset, and the tunnel endpoint ID (TEID) for both the SGSN and GGSN. The TEID is a unique number, much like a session ID on a TCP/IP firewall. All this information ensures a uniquely identifiable connection is made.

Since one mobile device may have multiple connections open at one time, such as data connections to different internet services and voice connections to different locations, there may be more than one PDP context with the same IP address making the extra identifying information required.

The endpoint that the mobile phone is connecting to only knows about the GGSN — the rest of the GPRS connection is masked by the GGSN.

Along the PDP context path, communication is accomplished in using three different protocols.

- The connection between the Mobile Station and SGSN uses the SM protocol.
- Between SGSN and GGSN GTP is used.
- Between GGSN and the endpoint IP is used.

FortiOS Carrier is concerned with the SGSN to GGSN part of the PDP context — the part that uses GTP.

## Creating a PDP context

While FortiOS Carrier is concerned mostly with the SGSN to GGSN part of the PDP Context, knowing the steps involved in creating a PDP context helps understand the role each device, protocol, and message type plays.

Both mobile stations and GGSNs can create PDP contexts.

### A Mobile Station creates a PDP context

1. The Mobile Station (MS) sends a `PDP activation request` message to the SGSN including the MS PDP address, and APN.
2. Optionally, security functions may be performed to authenticate the MS.
3. The SGSN determines the GGSN address by using the APN identifier.
4. The SGSN creates a down link GTP tunnel to send IP packets between the GGSN and SGSN.
5. The GGSN creates an entry in its PDP context table to deliver IP packets between the SGSN and the external packet switching network.
6. The GGSN creates an uplink GTP tunnel to route IP-PDU from SGSN to GGSN.
7. The GGSN then sends back to the SGSN the result of the PDP context creation and if necessary the MS PDP address.
8. The SGSN sends an `Activate PDP context accept` message to the MS by returning the negotiated PDP context information and if necessary the MS PDP address.
9. Now traffic can pass from the MS to the external network endpoint.

### A GGSN creates a PDP context

1. The network receives an IP packet from an external network.
2. The GGSN checks if the PDP Context has already been created.
3. If not, the GGSN sends a `PDU notification request` to the SGSN in order to initiate a PDP context activation.
4. The GGSN retrieves the IP address of the appropriate SGSN address by interrogating the HLR from the IMSI identifier of the MS.
5. The SGSN sends to the MS a request to activate the indicated PDP context.
6. The PDP context activation procedure follows the one initiated by the MS. See "A Mobile Station creates a PDP context".
7. When the PDP context is activated, the IP packet can be sent from the GGSN to the MS.

## Terminating a PDP context

A PDP context remains open until it is terminated. To terminate the PDP context an MS sends a `Deactivate PDP context` message to the SGSN, which then sends a `Delete PDP Context` message to the GGSN. When the SGSN receives a PDP context deletion acknowledgment from the GGSN, the SGSN confirms to the MS the PDP context deactivation. The PDP can be terminated by the SGSN or GGSN as well with a slight variation of the order of the messages passed.

When the PDP Context is terminated, the tunnel it was using is deleted as well. If this is not completed in a timely manner, it is possible for someone else to start using the tunnel before it is deleted. This hijacking will result in the original customer being over billed for the extra usage. Anti-overbilling helps prevent this.

# GPRS security

The GPRS network has some built-in security in the form of GPRS authentication. However this is minimal, and is not sufficient for carrier network security needs. A GTP firewall, such as FortiOS Carrier, is required to secure any GTP interface (Gi, Gn, S5, S8, S11, S2a/S2b, and so on).

## GPRS authentication

GPRS authentication is handled by the SGSN to prevent unauthorized GPRS calls from reaching the GSM network beyond the SGSN (the base station system, and mobile station). Authentication is accomplished using some of the customer's information with a random number and uses two algorithms to create ciphers that then allow authentication for that customer.

User identity confidentiality ensures that customer information stays between the mobile station and the SGSN — no identifying information goes past the SGSN. Past that point other numbers are used to identify the customer and their connection on the network.

Periodically the SGSN may request identity information from the mobile station to compare to what is on record, using the IMSI or T-IMSI number.

Call confidentiality is achieved through the use of a cipher, similar to the GPRS authentication described earlier. The cipher is applied between the mobile station and the SGSN. Essentially a cipher mask is XORd with each outgoing frame, and the receiving side XORs with its own cipher to result in the original frame and data.

# Radio access

For a mobile phone or user equipment (called a mobile station (MS)) to access the GPRS core network, it must first connect to the Radio Access Network (RAN). How the MS connects to the RAN is determined by what Radio Access Technologies (RATs) are supported by the RAN.

# Transport protocols

Transport protocols move data along the carrier network between radio access and the internet or other carrier networks.

FortiOS Carrier should be present where information enters the Carrier network, to ensure the information entering is correct and not malicious. This means FortiOS Carrier intercepts the data coming from the SGSN or foreign networks destined for the SSGN or GGSN onto the network. FortiOS Carrier should also intercept traffic that leaves the GGSN before it leaves the network.

## GTP

GPRS Tunneling Protocol (GTP) is a group of IP-based communications protocols used to carry General Packet Radio Service (GPRS) within Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) networks. GTP employs tunneling to transport GPRS packets over IP networks. This tunneling allows users to move between SGSNs and still maintain connection to the Internet through the GGSN.

GTP has three versions version 0, 1, and 2. GTPv1 and GTP2v are supported by FortiOS Carrier. The only GTP commands that are common to all forms of GTP are the echo request/response commands that allow GSNs to verify up to once every 60 seconds that neighboring GSNs are alive.

## GTPv0

The original version of GTP (version 0) has the following differences from version GTPv1.

- the tunnel identification is not random
- there are options for transporting X.25
- the fixed port number 3386 is used for all functions, not just charging
- optionally TCP is allowed as a transport instead of UDP
- not all message types are supported in version 0

## GTPv1

On a GPRS network, Packet Data Protocol (PDP) context is a data structure used by both the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). The PDP context contains the subscribers information including their access point, IP address, IMSI number, and their tunnel endpoint ID for each of the SGSN and GGSN.

The Serving GPRS Support Node (SGSN) is responsible for the delivery of data packets from and to the mobile stations within its geographical service area. Its tasks include packet routing and transfer, mobility management (attach/detach

and location management), logical link management, and authentication and charging functions. The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles (e.g., IMSI, address(es) used in the packet data network) of all GPRS users registered with this SGSN.

## GTPv1-C

GTPv1-C refers to the control layer of the GPRS Transmission network. This part of the protocol deals with network related traffic.

FortiOS Carrier handles GTPv1-C by using the Tunnel Endpoint IDentifier (TEID), IP address, and a Network layer Service Access Point Identifier (NSAPI), sometimes called the application identifier, as an integer value that is part of the PDP context header information used to identify a unique PDP context in a mobile station, and SGSN.

## GTPv1-U

GTPv1-U is defined in 3GPP TS 29.281 and refers to the user layer of the GPRS Tunneling network. This part of the protocol deals with user related traffic, user tunnels, and user administration.

A GTPv1-U tunnel is identified by a TEID, an IP address, and a UDP port number. This information uniquely identifies the limb of a GTPv1 PDP context. The IP address and the UDP port number define a UDP/IP path, a connectionless path between two endpoints (SGSN or GGSN). The TEID identifies the tunnel endpoint in the receiving GTPv1-U protocol entity; it allows for the multiplexing and demultiplexing of GTP tunnels on a UDP/IP path between a given GSN-GSN pair. For more information on GTPv1-U, see GTP-U messages.

The GTP core network consists of one or more SGSNs and GGSNs.

## GGSN

The Gateway GPRS Support Node (GGSN) connects the GPRS network on one side via the SGSN to outside networks such as the Internet. These outside networks are called packet data networks (PDNs). The GGSN acts as an edge router between the two different networks — the GGSN forwards incoming packets from the external PDN to the addressed SGSN and the GGSN also forwards outgoing packets to the external PDN. the GGSN also converts the packets from the GPRS packets with SGSN to the external packets, such as IP or X.25.

## SGSN

The Serving GPRS Support Node (SGSN) connects the GPRS network to GTPv1 compatible mobile stations, and mobile units (such as UTRAN and ETRAN) on one side and to the gateway node (GGSN), which leads to external networks, on the other side. Each SGSN has a geographical area, and mobile phones in that area connect to the GPRS network through this SGSN. The SGSN also maintains a location register that contains customer's location and user profiles until they connect through a different SGSN at which time the customer information is moved to the new SGSN. This information is used for packet routing and transfer, mobility management also known as location management, logical link management, and authentication and billing functions.

## GTPv2 / GTPv2-C

GTPv2, defined in 3GPP TS 29.274, is dramatically different from GTPv1, defined in 3GPP TS 29.060.

GTPv2-C is the control layer messaging for GTPv2. It is used by LTE mobile stations, SGSN units for backwards compatibility, and SGWs that are the gateway to other networks. In general the SGW manages the user data (GTP-U) and communicates with GTP-C via S11 with the MME for mobility management and with GTP-C via S5/S8 with the PGW for tunnel management. Also GTP (S2b in EMEA) is used between ePDG and PGW for VoWifi.

For more information about GTPv2, see GTPv2 - evolving packet core architecture on page 9.

### MME

MME essentially fills the Authentication and Mobility Management role of the SGSN in a GTPv1 network — it is how the mobile stations gain access to the Carrier network.

## Billing and records

A major part of the GPRS network is devoted to billing. Customer billing requires enough information to identify the customer, and then billing specific information such as connection locations and times, as well as amount of data transferred. A modified form of GTP called GTP' is used for billing. The home location records and visitor location records store information about customers that is critical to billing.

### GTP' (GTP prime)

GTP is used to handle tunnels of user traffic between SGSNs and GGSNs. However for billing purposes, other devices that are not supported by GTP are required. GTP' (GTP prime) is a modified form of GTP and is used to communicate with these devices such as the Charging Data Function (CDF) that communicates billing information to the Charging Gateway Function (CGF). In most cases, GTP' transports user records from many individual network elements, such as the GGSNs, to a centralism computer which then delivers the charging data more conveniently to the network operator's billing center, often through the CGF. The core network sends charging information to the CGF, typically including PDP context activation times and the quantity of data which the end user has transferred.

GTP' is used by the Ga and Gz interfaces to transfer billing information. GTP' uses registered UDP/TCP port 3386. GTP' defines a different header, additional messages, field values, as well as a synchronization protocol to avoid losing or duplicating CDRs on CGF or SGSN/GGSN failure. Transferred CDRs are encoded in ASN.1.

### HLR

The Home Location Register (HLR) is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network. There can be several logical, and physical, HLRs per public land mobile network (PLMN), though one international mobile subscriber identity (IMSI)/MSISDN pair can be associated with only one logical HLR (which can span several physical nodes) at a time. The HLRs store details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI which is the primary key to each HLR record.

### HSS

The Home Subscriber Server (HSS) combines the HLR and the Authentication Center (AuC) functions. The HLR stores and updates the database containing all the user subscription information, including the following:

- User identification and addressing, similar to the International Mobile Subscriber Identity (IMSI) and Mobile Subscriber ISDN Number (MSISDN) or mobile telephone number.
- User profile information, includes service subscription states and user-subscribed Quality of Service information (such as maximum allowed bit rate or allowed traffic class).

The generates security information from user identity keys and provides this information to the HLR and to other entities in the network. Security information is used for:

- Mutual network-terminal authentication.
- Radio path ciphering and integrity protection, to ensure data and control information transmitted between the network and the terminal is not eavesdropped or altered.

### VLR

The Visitor Location Register (VLR) is a database which stores information about all the mobile devices that are currently under the jurisdiction of the Mobile Switching Center which it serves. Of all the information the VLR stores about each Mobile Station, the most important is the current Location Area Identity (LAI). This information is vital in the call setup process.

Whenever an MSC detects a new MS in its network, in addition to creating a new record in the VLR, it also updates the HLR of the mobile subscriber, informing it of the new location of that MS.

## GPRS network common interfaces

There are interfaces for each connection on the GPRS network. An interface is an established standard form of communication between two devices. Consider a TCP/IP network. In addition to the transport protocol (TCP) there are other protocols on that network that describe how devices can expect communications to be organized, just like GPRS interfaces.

There are a series of interfaces that define how different devices on the carrier network communicate with each other. There interfaces are called Ga to Gz, and each one defines how a specific pair of devices will communicate. For example, Gb is the interface between the base station and the SGSN, and Gn is one possible interface between the SGSN and GGSN.

The SGSN and GGSN keep track of the CDR information and forward it to the Charging Data Function (CDF) using the Gr interface between the SGSN and home location register (HLR), Gs interface between the SGSN and MSC (VLR), Gx interface between the GGSN and the Charging Rules Function (CRF), Gy between the GGSN and online charging system (OCS), and finally Gz which is the off-line (CDR-based) charging interface between the GSN and the CG that uses GTP'.

Each of these interfaces on the GPRS network is has a name in the format of `Gx` where `x` is a letter of the alphabet that determines what part of the network the interface is used in. It is common for network diagrams of GPRS networks to include the interface name on connections between devices.

FortiOS Carrier provides protection on the Gn, Gp, and Gi interfaces.

**GPRS network interfaces, their roles, and billing**

| Name | Device connections that use this interface | Traffic Protocol used | Its role or how it affects billing |
|---|---|---|---|
| **Ga** | CDR and GSN (SGSNs and GGSNs) | GTP' - GTP modified to include CDR role | CDR have the accounting records, that are compiled in the GSN and then sent to the Charging Gateway (CG) |
| **Gb** | MS and SGSN | Frame Relay or IP | When an IP address moves to a new MS, the old MS may continue to use and bill that IP address. |
| **Gi** | GGSN and public data networks (PDNs) | IP based | This is the connection to the Internet. If the GTP tunnel is deleted without notifying the Gi interface, the connection may remain open incurring additional charges. FortiOS Carrier adds this interface to a firewall. See Anti-overbilling with FortiOS Carrier. |
| **Gn** | SGSN and external SGSNs and internal GGSNs | GTP | When the GTP tunnel is deleted, need to inform other interfaces immediately to prevent misuse of connections remaining open. FortiOS Carrier adds this interface to a firewall. |
| **Gp** | Internal SGSN and external GGSNs | GTP | |
| **Gz** | GSN (SGSN and GGSN) and the charging gateway (CG) | GTP' | Used for the offline charging interface. Ga is used for online charging. |

Corporate customers may have a direct connection to the Gi interface for higher security. The Gi interface is normally an IP network, though a tunneling protocol such as GRE or IPsec may be used instead.

# GTP as a Potential Attack Vector

GTP's role in transferring data in the core mobile infrastructure makes it a potential ideal attack vector. To understand the security features for GTP we need to understand the risks that might compromise this protocol. Attacks can include Denial of Service (DoS) attacks that reduce network performance due to resource starvation and remote compromise attacks that allow an outsider to gain remote control of a critical device (for example – take control over a GGSN of PGW).

GTP-based attacks may have a wide range of business impact, based on the attacked devices' vulnerability, ranging from service unavailability, compromise customer information, and gaining control over infrastructure elements, just to give a few examples.

Listed below are the main categories of GTP-based attacks:

- **Protocol anomaly attacks** are packets and packets formats that should not be expected on the GTP protocol. These can include malformed packets, reserved packets' fields and types, etc.
- **Infrastructure attacks** are attempts to connect to restricted core elements, such as the GGSN, SGSN, SGW, PGW, ePDG, etc.
- **Overbilling attacks** results in customers charged for traffic they did not use or the opposite of not paying for the used traffic.

## Protecting Against GTP-Based Attacks: The Carrier Grade GTP Firewall

With the evolution of the mobile network so has GTP evolved. The awareness to the potential of GTP-based attacks has led mobile core vendors to harden their software to better deal with potential attacks. Alongside this evolution, network security vendors, such as Fortinet, have led the way in providing GTP-aware firewalls to secure and protect the different versions of the GTP protocol from potential attacks.

A GTP firewall should be placed where GTP traffic and sessions originate and terminate, and has to inspect both the GTP-C (Control Plane) and GTP-U (Data Plane) packets that, together, constitute the GPRS Tunneling Protocol.

For example, the GTP firewall could be placed in line between the SGSN / SGW and the GGSN / PGW which are the initiator and terminator of the GTP traffic. One of the main roles of GTP firewalls is also to be able to support roaming between different versions of GTP without interrupting the service.

The GTP firewall must be carrier grade in its ability to scale and provide high availability without impact its ability to provide effective protection.

The most relevant GTP-related security documents published by the GSMA are FS.20 GTP Security and FS.37 GTP-U Security.

## FortiOS Carrier GTP protection

FortiOS Carrier is the part of FortiOS which was specifically designed to provide security for carriers and mobile operators' protocols and requirements, such as awareness and security for GTP. The wide range of FortiGate platforms with FortiOS and FortiOS Carrier enables mobile operators to cost effectively secure their mobile network against GTP-based attacks, while ensuring unparalleled performance, availability and security effectiveness.

# Packet sanity checking

The FortiOS Carrier checks the following items to determine if a packet confirms to the UDP and GTP standards:

- GTP release version number — must be 0, 1, or 2
- Settings of predefined bits
- Protocol type
- UDP packet length

If the packet in question does not confirm to the standards, the FortiOS Carrier firewall drops the packet, so that the malformed or forged traffic will not be processed.

# GTP stateful inspection

Apart from static inspection (checking the packet header), FortiOS Carrier performs stateful inspection.

Stateful inspection provides enhanced security by keeping track of communications sessions and packets over a period of time. Both incoming and outgoing packets are examined. Outgoing packets that request specific types of incoming packets are tracked; only those incoming packets constituting a proper response are allowed through the firewall.

When you add a GTP profile to a FortiOS Carrier firewall policy, the firewall also indexes GTP tunnels to keep track of them. Firewall policies that include a GTP profile can block unwanted encapsulated traffic in GTP tunnels, such as infrastructure attacks. Infrastructure attacks involve attempts by an attacker to connect to restricted machines, such as GSN devices, network management systems, or mobile base stations. If these attempts to connect are detected, they are flagged immediately by the firewall.

# Virtual domain support

FortiOS Carrier is suited to both large and smaller carriers. A single Carrier-enabled FortiGate unit can serve either one large carrier, or several smaller ones through virtual domains. As with any FortiGate unit, Carrier-enabled units have the ability to split their resources into multiple virtual units. This allows smaller carriers to use just the resources that they need without wasting the extra. For more information on HA in FortiOS, see the Virtual Domains (VDOMs) Guide.

# GTP stats via SNMP

All parameters/values that can be checked with the following debug commands are available via SNMP:

- `diagnose firewall gtp stat`
- `diagnose firewall gtp runtime-stat`

The following OID was added to make GTP stats available via SNMP:

- `1.3.6.1.4.1.12356.101.5.3`

The sequence of printed items of the debug commands was also adjusted to make it consistent with the data type and SNMP.

# FGCP GTP tunnel synchronization

FortiGate Clustering Protocol (FGCP) HA provides failover protection for GTP tunnels. This means that an active-passive cluster of two FortiGates licensed for FortiOS Carrier can provide FortiOS Carrier firewall services even when one of the FortiGates in the cluster encounters a problem that would result in complete loss of connectivity for a standalone FortiGate. This failover protection provides a backup mechanism that can be used to reduce the risk of unexpected downtime, especially for mission-critical environments.

Fortinet recommends FGCP GTP tunnel synchronization for an active-passive FGCP cluster of two FortiGates.

FGCP HA can be configured to synchronize TCP and UDP sessions. However synchronizing a session is only part of the solution if the goal is to continue GTP processing on a synchronized session after an HA failover. For that to be successful, FortiOS Carrier also synchronizes the GTP tunnel state. So, once the primary FortiGate in the FGCP cluster completes tunnel setup, the GTP tunnel is synchronized to the secondary or backup FortiGate in the cluster. GTP tunnel synchronization includes synchronizing all GTP tunnel information including session timers.

GTP traffic will only flow without interruption after an HA failover if bidirectional GTP policies have been configured: an internal (GTP server) to external (all) UDP port GTP policy, and an external (all) to internal (GTP server) UDP port GTP policy. If either policy is missing then traffic may be interrupted until traffic flows in the opposite direction.

For more information about HA in FortiOS, see High Availability.

# FGSP GTP tunnel synchronization

You can use the FortiGate Session Life Support Protocol (FGSP) to synchronize GTP tunnels between two FortiGates licensed for FortiOS Carrier. The FortiGates can be at the same location or distributed to different locations (for example, each FortiGate can be at a different data center). FGSP tunnel synchronization uses the same methods as FGCP GTP tunnel synchronization. All relevant GTP tunnel information is synchronized, including session timers.

Fortinet recommends FGSP GTP tunnel synchronization for an FGSP cluster of two FortiGates.

No special FGSP configuration is required for GTP tunnel synchronization. For information about configuring FGSP, see FGSP (session synchronization) peer setup.

In addition to GTP tunnel synchronization, in most cases you would want all of the FortiGates in the FGSP configuration to maintain the same configuration. If you want to synchronize configuration changes, consider enabling Using standalone configuration synchronization. You can also use FortiManager to manage and synchronize the configurations of the FortiGates.

Using FGSP to synchronize GTP tunnels between FGCP clusters supports asymmetric routing . Enter the following command to enable asymmetric routing:

```
config system settings
   set gtp-asym-fgsp enable
end
```

The FGSP supports widely separated FGSP peers installed in different physical locations. In a distributed FGSP cluster, session synchronization and HA heartbeat communication between FGSP peers can take place over the internet or over other transmission methods including satellite linkups.

Most Data Center Interconnect (DCI) or MPLS-based solutions that support layer 2 extensions between the remote data centers should also support FGSP heartbeat communication and session synchronization between FortiGates in the distributed locations.

Because of the possible distance, it may take a relatively long time for heartbeat packets to be transmitted between distributed FGSP peers. To account for possible delays, you can increase the FGSP heartbeat interval so that the FGSP peers expect extra time between heartbeat packets. A general rule is to configure the heartbeat time to be longer than the max latency.

You could also increase the number of lost heartbeat packets allowed before a FortiGate assumes an FGSP peer is offline if the network connection is less reliable.

Using the following command to adjust the FGSP heartbeat interval and number of lost packets. You can configure a custom heartbeat interval and lost packet threshold for each FGSP session synchronization instance.

```
config system cluster-sync
   edit <id>
      set hb-interval <interval>
      set hb-lost-threshold <threshold>
   end
```

`hb-interval <interval>` the heartbeat interval in seconds. The range 1 to 10 seconds and the default is 2 seconds.

`hb-lost-threshold <threshold>` the number of expected heartbeat packets to loose before assuming the FGSP peer is down. The range is 1 to 10 lost heartbeat packets and the default is 3 lost heartbeat packets.

You can also use different link paths for different session sync instances to optimize GTP tunnel synchronization performance. You could also configure QoS on the session synchronization links to make sure FGSP communication has the highest priority.

# Configuring GTP profiles

GTP profiles allow you to apply multiple types of filtering and content checking to GTP traffic passing through FortiOS Carrier. This section describes how to create and customize GTP profiles.

Once you have created GTP profiles, you can create firewall policies that accept the GTP traffic that you want to apply the GTP profile to.

To configure GTP profiles from the CLI, use the following command:

```
config firewall gtp
   edit <name>
      set ...
   end
```

To configure GTP profiles from the GUI, go to **Security Profiles > GTP Profiles**.

## General GTP profile settings

The following general settings are available when creating and editing GTP profiles from the CLI.

A subset of these settings is also available when editing a GTP profile on the GUI. To configure GTP profile general settings from the GUI, edit a GTP profile and open **General Settings**.

```
config firewall gtp
   edit <name>
      set gtp-in-gtp {allow | deny}
      set min-message-length <length>
      set max-message-length <length>
      set tunnel-limit <number-of-tunnels>
      set tunnel-timeout <time>
      set control-plane-message-rate-limit <packets-per-second>
      set handover-group <firewall-address>
      set authorized-sgsns <firewall-address>
      set invalid-sgsns-to-log <firewall-address>
      set authorized-ggsns <firewall-address>
      set remove-if-echo-expires (disable | enable}
      set remove-if-recovery-differ (disable | enable}
      set send-delete-when-timeout (disable | enable}
      set send-delete-when-timeout-v2 (disable | enable}
      set unknown-version-action {allow | deny}
      set echo-request-interval <time>
      set half-open-timeout <timeout>
      set half-close-timeout <timeout>
      set monitor-mode {disable | enable | vdom}
   end
```

| Option | Description |
|---|---|
| `gtp-in-gtp` | On the GUI: **General Settings > GTP-in-GTP**. Select `allow` to enable GTP packets to be allowed to contain GTP packets, or a GTP tunnel inside another |

| Option | Description |
|---|---|
| | GTP tunnel. To block all GTP-in-GTP packets, select `deny`. |
| `min-message-length`<br>`max-message-length` | On the GUI: **General Settings >Message length**. Define the acceptable message size range in bytes. Normally this is controlled by the protocol, and will vary for different message types. If a packet is smaller or larger than this range, it is discarded as it is likely malformed and a potential security risk. The default ranges is 0 to 1452 bytes. |
| `tunnel-limit` | On the GUI: **General Settings > Tunnel limit**. See GTP tunnel limiting on page 25. |
| `tunnel-timeout` | On the GUI: **General Settings > Tunnel timeout**. Enter the maximum number of seconds that a GTP tunnel is allowed to remain active. After the timeout, FortiOS Carrier deletes GTP tunnels that have stopped processing data. A GTP tunnel may hang for various reasons. For example, during the GTP tunnel tear-down stage, the d`elete pdap context response` message may get lost. By setting a timeout value, FortiOS Carrier will remove hanging tunnels. The default is 86400 seconds, or 24 hours. |
| `control-plane-message-rate-limit` | On the GUI: **General Settings > Control plane message rate limit**. Enter the number of packets per second to limit the traffic rate to protect the GSNs from possible Denial of Service (DoS) attacks. The default limit of 0 does not limit the message rate. GTP DoS attacks can include: **Border gateway bandwidth saturation**: A malicious operator can connect to your IPX/GRX and generate high traffic towards your Border Gateway to consume all the bandwidth. **GTP flood**: A GSN can be flooded by illegitimate traffic |
| `handover-group` | On the GUI: **General Settings > Handover group**. Select the firewall address that contains the list of IP addresses allowed to take over a GTP session when the mobile device moves locations. Handover is a fundamental feature of GPRS/UMTS, which enables subscribers to seamlessly move from one area of coverage to another with no interruption of active sessions. Session hijacking can come from the SGSN or the GGSN, where a fraudulent GSN can intercept another GSN and redirect traffic to it. This can be exploited to hijack GTP tunnels or cause a denial of service. When the handover group is defined it acts like an allow list with an implicit default deny at the end — the GTP address must be in the group or the GTP message will be blocked. This stops handover requests from untrusted GSNs. |
| `authorized-sgsns` | On the GUI: **General Settings > Authorized SGSNs**. Select a firewall address that only allows authorized SGSNs and SGWs that match the firewall address to send packets through FortiOS Carrier and to block unauthorized SGSNs and SGWs. You can use authorized SGSNs to allow packets from SGSNs or SGWs that have a roaming agreement with your organization. |
| `invalid-sgsns-to-log` | Select a firewall address to match invalid SGSNs and record an invalid SGSN log message when a matching invalid SGSN is found. |
| `authorized-ggsns` | On the GUI: **General Settings > Authorized GGSNs**. Select a firewall address that only allows authorized GGSNs or PGWs to send packets through the unit and |

| Option | Description |
|---|---|
| | to block unauthorized GGSNs. You can use authorized GGSNs or PGWs to allow packets from GGSNs or PGWs that have a roaming agreement with your organization. |
| `remove-if-echo-expires` | Enable to remove sessions if the echo response expires. Disabled by default. |
| `remove-if-recovery-differ` | Enable to remove a session if the recovery IE is different. Disabled by default. |
| `send-delete-when-timeout` | Enable to send a DELETE request to path endpoints when a GTPv0/v1 tunnel times out. Disabled by default. |
| `send-delete-when-timeout-v2` | Enable to send a DELETE request to path endpoints when a GTPv2 tunnel times out. Disabled by default. |
| `unknown-version-action` | Allow or deny sessions with unknown GTP versions. Unknown GTP versions are allowed by default. |
| `echo-request-interval` | Set the amount of time to wait for an echo request. The default is 0, which means no limit on the amount of time to wait for an echo request. |
| `half-open-timeout` | Set the half-open timeout in seconds for GTP sessions. The range is 1 to 300 and the default is 300. This option allows you to use the GTP profile to customize the half-open timer for GTP sessions. |
| `half-close-timeout` | Set the half-close timeout in seconds for GTP sessions. The range is 1 to 30 and the default is 10. This option allows you to use the GTP profile to customize the half-close timer for GTP sessions. |
| `monitor-mode` | Set the GTP monitor mode for all GTP versions. You can enable or disable global monitoring mode or select `vdom` (the default) to select monitoring mode per VDOM.<br>When enabled, if a GTP packet is to be dropped due to a GTP deny case such as:<br>• GTP_DENY<br>• GTP_RATE_LIMIT<br>• GTP_STATE_INVALID<br>• GTP_TUNNEL_LIMIT<br>instead of being dropped, it will be forwarded and logged with the original deny log message and a `-monitor` suffix (for example, `state-invalid-monitor`). |

# GTP tunnel limiting

FortiOS Carrier includes two methods for limiting the number of GTP tunnels that can be operating at one time.

- You can add a tunnel limit to a GTP profile. All traffic processed by that GTP profile cannot open more tunnels than this configured tunnel limit.
- You can create global tunnel limits and add these tunnel limits to GTP profiles. This global tunnel limit applies to all traffic processed by all of the GTP profiles configured with that same global tunnel limit.

You can combine both methods of tunnel limiting in the same GTP profile. If you do this, the two tunnel limiting features keep separate track of the number of tunnels, and the number of tunnels allowed is limited by the first limiter to reach its limit.

Limiting the number of GTP tunnels can help prevent a form of denial of service attack on your network. This attack involves opening more tunnels than the network can handle and consuming extra network resources. By limiting the number of tunnels at any one time, this form of attack will be avoided.

## GTP profile tunnel limit

Use the following command to set the tunnel limit for a GTP profile:

```
config firewall gtp
   edit <name>
      set tunnel-limit <number-of-tunnels>
   end
```

On the GUI: **General Settings > Tunnel limit**.

Enter the maximum number of tunnels allowed to be open at one time. The range is 1 16000000 tunnels. The default tunnel limit is 0, which means no limit.

## Global GTP tunnel limits

Use the following command to create global shared tunnel limits:

```
config gtp tunnel-limit
   edit <global-tunnel-limit-name>
      set tunnel-limit <number-of-tunnels>
   end
```

Enter the maximum number of global tunnels allowed to be open at one time. The range is 1 16000000 tunnels. The default limit is 0, which means no limit.

You can add multiple global tunnel limits. Global tunnel limits are added to a VDOM and can be applied to traffic processed by that VDOM

Use the following command to add a shared tunnel limit to a GTP profile:

```
config firewall gtp
   edit <profile-name>
      set global-tunnel-limit <global-tunnel-limit-name>
   end
```

You can use the following diagnose command to view information about global tunnel limits.

```
diagnose firewall gtp tunnel-limit list
```

The command output includes a line for each global tunnel limit. The output includes the name of the tunnel limit, its configured limit, and the number of tunnels processed by GTP profiles that the global tunnel limit has been added to. For example:

```
name=gtp-tl-1 tunnel_limit=7000 tunnel_count=500
```

# APN traffic shaping

You can configure APN traffic shaping to control the number of GTP tunnels per second created by FortiOS Carrier. If your FortiOS Carrier includes multiple VDOMS, you can create an APN traffic shaping configuration for each VDOM. APN traffic shaping only applies to traffic accepted by firewall policies with GTP profiles but applies to all GTP traffic processed by GTP profiles.

APN traffic shaping allows you to create a list of APN traffic shaping policies. The policies allow you to control how many GTP tunnels per second FortiOS Carrier will create for each of the APNs in the policy list. You can configure the policy to either drop or reject packets that exceed the configured rate.

You can also create a general APN traffic shaping policy with no APNs to apply traffic shaping to GTP traffic with any APN. This allows you to limit the number of tunnels per second created by all GTP traffic.

Just like firewall policies, FortiOS carrier reads the APN traffic shaping list in ascending order by policy ID and applies traffic shaping based on the first matching APN. One way to configure APN traffic shaping would be to create a general APN traffic shaping policy with a blank APN field. Give this policy a relatively high policy ID. Then add policies with lower policy IDs that contain specific APNs so that they appear higher in the list.

Creating a general APN traffic shaping policy is not required. If you don't create a general policy, traffic with APNs that don't match APNs in the policy list are not limited by APN traffic shaping.

Use the following command to create an APN traffic shaping policy list:

```
config gtp apn-shaper
   edit <policy-id>
      set apn [<apn-name> <apngrp-name> ...]
      set rate-limit <limit>
      set action {drop | reject}
      set back-off-time <time>
   end
```

`apn` select one or more APNs created with the `config gtp apn` command and one or more APN groups created with the `config gtp apngrp` command. You can also leave this blank to apply the shaper to any APN.

`rate-limit` enter the rate limit in the range 0 to 1000000 packets per second. 0, the default, means unlimited. The rate limit refers to the number of GTP tunnel creation packets that FortiOS Carrier accepts per second, effectively limiting the GTP tunnel creation rate.

`action` can be `drop` or `reject`.

- `drop` drops the packet
- `reject` performs a GTP reject action which returns an APN congestion packet with a back-off timer. GTPv0 does not support back-off timers so the reject action is not supported for GTPv0 packets. The reject action with back-off timer is supported for GTPv1 and GTPv2.

`back-off-time` if you set `action` to `reject`, specify a back-off time in seconds in the range of 10 to 360. The default is 0 but must be changed to be within the valid range.

You can use the following diagnose command to view the APN traffic shaper policy list, including the order of the policies in the list.

```
diagnose firewall gtp vd-apn-shaper list
```

## Supporting sub-second sampling

By default, the APN shaper samples traffic every second. In some cases, you may want to sample traffic more often. You can do this by enabling sub-second sampling in a GTP profile and setting the sub second sampling interval.

The following command enables sub-second sampling for a GTP profile and sets the sub-second sampling interface to 0.1 seconds:

```
config firewall gtp
   edit <name>
      set sub-second-sampling enable
      set sub-second-interval 0.1
   end
```

`sub-second-interval` can be 0.5, 0.25, or 0.1 seconds.

# GTPv0/v1 message filtering

FortiOS Carrier supports message filtering for all GTPv0/v1 message types as defined by 3GPP TS 29.060. Using GTPv0/v1 message filtering you can configure a GTP profile to allow or deny different types of GTPv0/v1 messages. All message types are allowed by default and you can create message filters to select message types to deny.

You can also use unknown message filtering to filter GTPv0v1 message types that FortiOS Carrier does not have message filtering options for. Unknown messages are usually new messages that are in use on your network but have only recently been added to GTPv0v1 by the 3GPP. These messages may be considered by the 3GPP as reserved or for future use.

You can set `unknown-message` to `deny` to block all unknown GTPv0/v1 message types. If you set `unknown-message` to `deny`, you can allow selected unknown message types by adding the IDs of these message types to the `unknown-message-white-list` option.

From the CLI, use the following command to add GTPv0/v1 message filtering to a GTP profile:

```
config firewall gtp
   edit <name>
      set message-filter-v0v1 <gtpv0v1-message-filter-name>
   end
```

Use the following command to create a GTPv0/v1 message filter:

```
config gtp message-filter-v0v1
   edit <name>
      set unknown-message {allow | deny}
      set unknown-message-white-list {1 2 ... 255}
      set echo {allow | deny}
      set version-not-support {allow | deny}
      set node-alive {allow | deny}
      set redirection {allow | deny}
      set create-pdp {allow | deny}
      set update-pdp {allow | deny}
      set delete-pdp {allow | deny}
      set v0-create-aa-pdp--v1-init-pdp-ctx {allow | deny}
      set delete-aa-pdp {allow | deny}
      set error-indication {allow | deny}
      set pdu-notification {allow | deny}
```

```
    set support-extension {allow | deny}
    set send-route {allow | deny}
    set failure-report {allow | deny}
    set note-ms-present {allow | deny}
    set identification {allow | deny}
    set sgsn-context {allow | deny}
    set fwd-relocation {allow | deny}
    set relocation-cancel {allow | deny}
    set fwd-srns-context {allow | deny}
    set ue-registration-query {allow | deny}
    set ran-info {allow | deny}
    set mbms-notification {allow | deny}
    set create-mbms {allow | deny}
    set update-mbms {allow | deny}
    set delete-mbms {allow | deny}
    set mbms-registration {allow | deny}
    set mbms-de-registration {allow | deny}
    set mbms-session-start {allow | deny}
    set mbms-session-stop {allow | deny}
    set mbms-session-update {allow | deny}
    set ms-info-change-notif {allow | deny}
    set data-record {allow | deny}
    set end-marker {allow | deny}
    set gtp-pdu {allow | deny}
end
```

From the GUI, create or edit a GTP profile, select **Message Filtering**, and select a message filter to add a GTPv0/v1 message filter to the profile.

To create a GTPv0/v1 message filter from the GUI, go to **Security Profiles > GTP Message Filters** and select **Create New > Message filter for GTPv0/v1**.

The following table lists FortiOS Carrier GTPv0v1 message filtering options and describes the GTPv0v1 message types and message IDs they apply to.

| Message filtering option | GTPv0/v1 message types and values |
|---|---|
| `echo` | Echo request (1) and Echo response (2). |
| `version-not-support` | Version not supported (3). |
| `node-alive` | Node alive request (4). Node alive response (5). |
| `redirection` | Redirection request (6). Redirection response (7). |
| `create-pdp` | Create PDP context request (16). Create PDP context response (17). |
| `update-pdp` | Update PDP context request (18). Update PDP context response (19). |
| `delete-pdp` | Delete PDP context request (20). Delete PDP context response (21). |
| `v0-create-aa-pdp--v1-init-pdp-ctx` | GTPv0: Create AA PDP context request (22). Create AA PDP context response (23).<br>or<br>GTPv1: Initiate PDP context activation request (22). Initiate PDP context activation response (23). |
| `delete-aa-pdp` | GTPv0: Delete AA PDP context request (24). Delete AA PDP context request |

| Message filtering option | GTPv0/v1 message types and values |
|---|---|
| | response (25). |
| error-indication | Error indication (26). |
| pdu-notification | PDU notification request (27). PDU notification response (28). Reject PDU notification request (29). Reject PDU notification response (30). |
| support-extension | GTPv1 Supported extension headers notify (31). |
| send-route | Send routing information for GPRS request (32). Send routing information for GPRS response (33). |
| failure-report | Failure report request (34). Failure report response (35). |
| note-ms-present | Note MS GPRS present request (36). Note MS GPRS present response (37). |
| identification | Identification request (48). Identification response (49). |
| sgsn-context | SGSN context request (50). SGSN context response (51). SGSN context ack (52). |
| fwd-relocation | GTPv1: Forward relocation request (53). Forward relocation response (54). Forward relocation complete (55). Forward relocation complete ack (59). |
| relocation-cancel | GTPv1: Relocation cancel request (56). Relocation cancel response (57). |
| fwd-srns-context | GTPv1: Forward SRNS context (58). Forward SRNS context ack 60). |
| ue-registration-query | UE Registration Query request (61). UE Registration Query response (62). |
| ran-info | GTPv1: RAN information relay (70). |
| mbms-notification | GTPv1: MBMS notification request (96). MBMS notification response (97). MBMS notification reject request (98). MBMS notification reject response (99). |
| create-mbms | GTPv1: Create MBMS context request (100) Create MBMS context response (101). |
| update-mbms | GTPv1: Update MBMS context request (102) Update MBMS context response (103). |
| delete-mbms | GTPv1: Delete MBMS context request (104). Delete MBMS context response (105). |
| mbms-registration | GTPv1: MBMS registration (request 112, response 113). |
| mbms-de-registration | GTPv1: MBMS de-registration request (114) MBMS de-registration response (115). |
| mbms-session-start | GTPv1: MBMS session start request (116). MBMS session start response (117). |
| mbms-session-stop | GTPv1: MBMS session stop request (118). MBMS session stop response (119). |
| mbms-session-update | GTPv1 MBMS session update request (120). MBMS session update response (121). |
| ms-info-change-notif | GTPv1: MS info change notification request (128). MS info change notification response (129). |

| Message filtering option | GTPv0/v1 message types and values |
|---|---|
| data-record | Data record transfer (request 240, response 241). |
| end-marker | GTPv1: End marker (254). |
| gtp-pdu | G-PDU (255). |

# GTPv2 message filtering

FortiOS Carrier supports message filtering for all GTPv2 message types as specified by 3GPP TS 29.274. Using GTPv2 message filtering you can configure a GTP profile to allow or deny different types of GTPv2 messages. All message types are allowed by default and you can create message filters to select messages to deny.

You can also use unknown message filtering to filter GTPv2 message types that FortiOS Carrier does not have message filtering options for. Unknown messages are usually new messages that are in use on your network but have only recently been added to GTPv2 by the 3GPP. These messages may be considered by the 3GPP as reserved or for future use.

You can set `unknown-message` to `deny` to block all unknown GTPv2 message types. If you set `unknown-message` to `deny`, you can allow selected unknown message types by adding the IDs of these message types to the `unknown-message-white-list` option.

For example, FortiOS Carrier does not have a message filter for message types 40 and 41: Remote UE Report Notification / Acknowledge. You can use the following configuration to create a GTPv2 message filter that denies unknown message types but allows message types 40 and 41:

```
config gtp message-filter-v2
   edit <name>
      set unknown-message deny
      set unknown-message-white-list 40 41
   end
```

From the CLI, use the following command to add GTPv2 message filtering to a GTP profile:

```
config firewall gtp
   edit <name>
      set message-filter-v2 <gtpv2-message-filter-name>
   end
```

Use the following command to create a GTPv2 message filter:

```
config gtp message-filter-v2
   edit <name>
      set unknown-message {allow | deny}
      set unknown-message-white-list {1 2 ... 255}
      set echo {allow | deny}
      set version-not-support {allow | deny}
      set create-session {allow | deny}
      set modify-bearer-req-resp {allow | deny}
      set delete-session {allow | deny}
      set change-notification {allow | deny}
      set remote-ue-report-notif-ack {allow | deny}
      set modify-bearer-cmd-fail {allow | deny}
      set delete-bearer-cmd-fail {allow | deny}
      set bearer-resource-cmd-fail {allow | deny}
```

```
    set dlink-notif-failure {allow | deny}
    set trace-session {allow | deny}
    set stop-paging-indication {allow | deny}
    set create-bearer {allow | deny}
    set update-bearer {allow | deny}
    set delete-bearer-req-resp {allow | deny}
    set delete-pdn-connection-set {allow | deny}
    set pgw-dlink-notif-ack {allow | deny}
    set identification-req-resp {allow | deny}
    set context-req-res-ack {allow | deny}
    set forward-relocation-req-res {allow | deny}
    set forward-relocation-cmp-notif-ack {allow | deny}
    set forward-access-notif-ack {allow | deny}
    set relocation-cancel-req-resp {allow | deny}
    set configuration-transfer-tunnel {allow | deny}
    set detach-notif-ack {allow | deny}
    set cs-paging {allow | deny}
    set ran-info-relay {allow | deny}
    set alert-MME-notif-ack Alert {allow | deny}
    set ue-activity-notif-ack {allow | deny}
    set isr-status {allow | deny}
    set ue-registration-query-req-resp {allow | deny}
    set create-forwarding-tunnel-req-resp {allow | deny}
    set suspend {allow | deny}
    set resume {allow | deny}
    set create-indirect-forwarding-tunnel-req-resp {allow | deny}
    set delete-indirect-forwarding-tunnel-req-resp {allow | deny}
    set release-access-bearer-req-resp {allow | deny}
    set dlink-data-notif-ack {allow | deny}
    set reserved-for-earlier-version {allow | deny}
    set pgw-restart-notif-ack {allow | deny}
    set update-pdn-connection-set {allow | deny}
    set modify-access-req-resp {allow | deny}
    set mbms-session-start-req-resp {allow | deny}
    set mbms-session-update-req-resp {allow | deny}
    set mbms-session-stop-req-resp {allow | deny}
  end
```

From the GUI, create or edit a GTP profile, select **Message Filtering**, and select a message filter to add a GTPv2 message filter to the profile.

To create a GTPv2 message filter from the GUI, go to **Security Profiles > GTP Message Filters** and select **Create New > Message filter for GTPv2**.

The following table lists FortiOS Carrier GTPv2 message type filtering options and describes the GTPv2 message types and message IDs they apply to.

| Message filtering option | GTPv2 message types and values |
|---|---|
| `echo` | Echo request (1). Echo response (2). |
| `version-not-support` | Version not supported (3). |
| `create-session` | Create session request (32). Create session response (33). |
| `modify-bearer-req-resp` | Modify bearer request (34). Modify bearer response (35). |

| Message filtering option | GTPv2 message types and values |
|---|---|
| delete-session | Delete session request (36). Delete session response (37). |
| change-notification | Change notification request (38). Change notification response (39). |
| remote-ue-report-notif-ack | Remote UE report notification (40). Remote UE report acknowledge (41). |
| modify-bearer-cmd-fail | Modify bearer command (64). Modify bearer failure indication (65). |
| delete-bearer-cmd-fail | Delete bearer command (66). Delete bearer failure indication (67). |
| bearer-resource-cmd-fail | Bearer resource command (68). Bearer resource failure indication (69). |
| dlink-notif-failure | Downlink data notification failure indication (70). |
| trace-session | Trace session activation (71). Trace session deactivation (72). |
| stop-paging-indication | Stop paging indication (73). |
| create-bearer | Create bearer request (95). Create bearer response (96). |
| update-bearer | Update bearer request (97). Update bearer response (98). |
| delete-bearer-req-resp | Delete bearer request (99). Delete bearer response (100). |
| delete-pdn-connection-set | Delete PDN connection set request (101). Delete PDN connection set response (102). |
| pgw-dlink-notif-ack | PGW downlink notification (103). PGW downlink acknowledge (104). |
| identification-req-resp | Identification request (128). Identification response (129). |
| context-req-res-ack | Context request (130). Context response (131). Context acknowledge (132). |
| forward-relocation-req-res | Forward relocation request (133). Forward relocation response (134). |
| forward-relocation-cmp-notif-ack | Forward relocation complete notification (135). Forward relocation complete acknowledge (136). |
| forward-access-notif-ack | Forward access context notification (137). Forward access context acknowledge (138). |
| relocation-cancel-req-resp | Relocation cancel request (139). Relocation cancel response (140). |
| configuration-transfer-tunnel | Configuration transfer tunnel (141). |
| detach-notif-ack | Detach notification (149). Detach acknowledge (150). |
| cs-paging | CS paging indication (151). |
| ran-info-relay | RAN information relay (152). |
| alert-MME-notif-ack | Alert MME notification (153). Alert MME acknowledge (154). |
| ue-activity-notif-ack | UE activity notification (155). UE activity Acknowledge (156). |

| Message filtering option | GTPv2 message types and values |
|---|---|
| isr-status | ISR status indication (157). |
| ue-registration-query-req-resp | UE registration query request (158). UE registration query response (159). |
| create-forwarding-tunnel-req-resp | Create forwarding tunnel request (160). Create forwarding tunnel response (161). |
| suspend | Suspend notify (162). Suspend acknowledge (163). |
| resume | Resume notify (164). Resume acknowledge (165). |
| create-indirect-forwarding-tunnel-req-resp | Create indirect data forwarding tunnel request (166). Create indirect data forwarding tunnel response (167). |
| delete-indirect-forwarding-tunnel-req-resp | Delete indirect data forwarding tunnel request (168). Delete indirect data forwarding tunnel response (169). |
| release-access-bearer-req-resp | Release access bearers request (170). Release access bearers response (171). |
| dlink-data-notif-ack | Downlink data notification (176). Downlink data acknowledge (177). |
| reserved-for-earlier-version | Reserved for earlier version of the GTP specification (178). |
| pgw-restart-notif-ack | PGW restart notification (179). PGW restart acknowledge (180). |
| update-pdn-connection-set | Update PDN connection set request (200). Update PDN connection set response (201). |
| modify-access-req-resp | Modify access bearers request (211). Modify access bearers response (212). |
| mbms-session-start-req-resp | MBMS session start request (231). MBMS session start response (232). |
| mbms-session-update-req-resp | MBMS session update request (233). MBMS session update response (234). |
| mbms-session-stop-req-resp | MBMS session stop request (235). MBMS session stop response (236). |

# GTPv0/v1 message rate limiting

In a GTP profile, you can use the following command to apply GTPv0/v1 message rate limiting.

```
config firewall gtp
   set rate-sampling-interval <interval>
   set rate-limit-mode {per-profile | per-stream | per-apn}
   set warning-threshold <percent>
   set user-plane-message-rate-limit 0
      edit <name>
```

```
config message-rate-limit
   set echo-request <limit>
   set echo-reponse <limit>
   set version-not-support <limit>
   set create-pdp-request <limit>
   set create-pdp-response <limit>
   set update-pdp-request <limit>
   set update-pdp-response <limit>
   set delete-pdp-request <limit>
   set delete-pdp-response <limit>
   set create-aa-pdp-request <limit>
   set create-aa-pdp-response <limit>
   set delete-aa-pdp-request <limit>
   set delete-aa-pdp-response <limit>
   set error-indication <limit>
   set pdu-notify-request <limit>
   set pdu-notify-response <limit>
   set pdu-notify-rej-request <limit>
   set pdu-notify-rej-response <limit>
   set support-ext-hdr-notify <limit>
   set send-route-request <limit>
   set send-route-response <limit>
   set failure-report-request <limit>
   set failure-report-response <limit>
   set note-ms-request <limit>
   set note-ms-response <limit>
   set identification-request <limit>
   set identification-response <limit>
   set sgsn-context-request <limit>
   set sgsn-context-response <limit>
   set sgsn-context-ack <limit>
   set fwd-relocation-request <limit>
   set fwd-relocation-response <limit>
   set fwd-relocation-complete <limit>
   set relocation-cancel-request <limit>
   set relocation-cancel-response <limit>
   set fwd-srns-context <limit>
   set fwd-reloc-complete-ack <limit>
   set fwd-srns-context-ack <limit>
   set ran-info <limit>
   set mbms-notify-request <limit>
   set mbms-notify-response <limit>
   set mbms-notify-rej-request <limit>
   set mbms-notify-rej-response <limit>
   set create-mbms-request <limit>
   set create-mbms-response <limit>
   set update-mbms-request <limit>
   set update-mbms-response <limit>
   set delete-mbms-request <limit>
   set delete-mbms-response <limit>
   set mbms-reg-request <limit>
   set mbms-reg-response <limit>
   set mbms-de-reg-request <limit>
   set mbms-de-reg-response <limit>
   set mbms-ses-start-request <limit>
   set mbms-ses-start-response <limit>
   set mbms-ses-stop-request <limit>
```

```
        set mbms-ses-stop-response <limit>
        set g-pdu <limit>
    end
```

`rate-sampling-interval` set how often, in seconds, to sample the rate. The range is 1 to 3600 and the default is 1 second.

`rate-limit-mode` select whether the rate limiting is applied `per-profile` (the default), `per-stream`, or `per-apn`.

`warning-threshold` set the rate limiting warning threshold in the range 0 to 99 percent. The default is 0 percent.

`<limit>` is the message limit in packets per second. The range is 0 to 4294967295. The default for all message types is 0, which is no rate limiting.

## GTPv2 message rate limiting

In a GTP profile, you can use the following command to apply GTPv2 message rate limiting.

```
config firewall gtp
   edit <name>
      config message-rate-limit-v2
         set echo-request <limit>
         set create-session-request <limit>
         set delete-session-request <limit>
      end
```

Where, `<limit>` is the message limit in packets per second. The range is 0 to 4294967295. The default for all message types is 0, which is no rate limiting.

## When to use APN, basic (IMSI), or policy (advanced) filtering

At first glance APN, IMSI, and advanced filtering have parts in common. For example, two can filter on APN, and another two can filter on IMSI. The difficulty is knowing when to use which type of filtering.

| Filtering type | Filter on the following data: | When to use this type of filtering |
|---|---|---|
| APN | APN | Filter based on GTP tunnel start or destination |
| Basic (IMSI) | IMSI, MCC-MNC | Filter based on subscriber information |
| Policy (Advanced) | PDP context, APN, IMSI, MSISDN, RAT type, ULI, RAI, IMEI | When you want to filter based on:<br>• user phone number (MSISDN)<br>• what wireless technology the user employed • to get on the network (RAT type)<br>• user location (ULI and RAI)<br>• handset ID, such as for stolen phones (IMEI) |

APN filtering is very specific — the only identifying information that is used to filter is the APN itself. This will always be present in GTP tunnel traffic, so all GTP traffic can be filtered using this value.

Basic (IMSI) filtering can use a combination of the APN and MCC-MNC numbers. The MCC and MNC are part of the APN, however filtering on MCC-MNC separately allows you to filter based on country and carrier instead of just the destination of the GTP Tunnel.

Policy (Advanced) filtering can go into much deeper detail covering PDP contexts/Sessions, MSISDN, IMEI, and more not to mention APN, and IMSI as well. If you can't find the information in APN or IMSI that you need to filter on, then use Advanced filtering.

# APN filtering

An Access Point Name (APN) is an Information Element (IE) included in the header of a GTP packet. APNs provide information about how to reach a network. An APN has the following format:

`<network_id>[.mnc<mnc_int>.mcc<mcc_int>.gprs]`

Where:

- `<network_id>` is a network identifier or name that identifies the name of a network, for example, `example.com` or `internet`.
- `[.mnc<mnc_int>.mcc<mcc_int>.gprs]` is the optional operator identifier that uniquely identifies the operator's PLMN, for example, `mnc123.mcc456.gprs`.

Combining these two examples results in a complete APN of `internet.mnc123.mcc456.gprs`.

By default, GTP profiles allow all APNs. You configure APN filtering to restrict the APNs that users can access.

You can APN filtering to GTP create pdp request messages (GTPv1) and create session request messages (GTPv2). FortiOS Carrier inspects GTP packets for both APN and selected modes. If both parameters match an APN filter entry, FortiOS Carrier applies the filter action the traffic.

Additionally, FortiOS Carrier can filter GTP packets based on the combination of an IMSI prefix and an APN.

## Creating APNs

Before adding APN filtering to a GTP profile you must create an APN. You can also combine multiple APNs into an APN group. Use the following command to create an APN group:

```
config gtp apn
   edit <apn-name>
      set apn <apn-value>
   end
```

The `<apn-value>` can include wild cards to match multiple APNs. For example `*.mcc333.mcn111.gprs` would match all APNs from country `333` and carrier `111` on the gprs network.

From the GUI, go to **Security Profiles > GTP APN** and select **Create New > GTP APN**. Add a **Name** for the APN and add an **APN Value**.

## Creating APN groups

Use the following command to create an APN group:

```
config gtp apngrp
```

```
edit <name>
   set member {apn1 apn2 ...}
end
```

From the GUI, go to **Security Profiles > GTP APN** and select **Create New > GTP APN Group**. Add a **Name** for the APN group and add **Group members** to it.

## Adding an APN filter to a GTP profile

Use the following command to add an APN to a GTP profile:

```
config firewall gtp
   edit <name>
      set apn-filter enable
      set default-apn-action {allow | deny}
         config apn
            edit <id>
               set apnmember <apn-name>
               set action {allow | deny}
               set selection-mode {ms | net | vrf}
            end
```

Set `default-apn-action` to `allow` to allow traffic, then use `config apn` to create APN filters to filter the allowed traffic. Set `default-apn-action` to `deny` to block all traffic and then use `config apn` to create APN filters that match the traffic to be allowed.

`<apn-name>` can be the name of an APN or an APN group.

`selection-mode` select one or more of the following APN modes. By default, all three modes are selected. The mode indicates where the APN originated and whether the Home Location Register (HLR) has verified the user subscription.

- `ms` MS-provided APN, subscription not verified, indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user's subscription to the network.
- `net` Network-provided APN, subscription not verified, indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user's subscription to the network.
- `sub` MS or Network-provided APN, subscription verified, indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network.

## APN filtering from the GUI

From the GUI:

1. Go to **Security Profiles > GTP Profiles**.
2. Add or edit a GTP profile and select **APN Filtering**.
3. Set the **Default APN Action**.
4. Select **Create New** to add an APN filter.
5. Select an APN or APN Group.
6. Select one or more of the available **Modes** to indicate where the APN or APN group originated and whether the Home Location Register (HLR) has verified the user subscription.
7. Set the **Action** to **Allow** or **Deny**.
8. Select **OK** to save the APN.
9. Select **Create New** to add more APNs.

# Basic filtering

You can use basic filtering in a GTP profile to allow or deny traffic based on APN, MCC-MNC, mode, and MSISDN. Basic filtering is also called IMSI filtering.

The International Mobile Station Identity (IMSI) is used by a GPRS Support Node (GSN) to identify a mobile station. Three elements make up every IMSI:

- the mobile country code (MCC)
- the mobile network code (MNC)
- the mobile subscriber identification number (MSISDN).

The subscriber's home network—the public land mobile network (PLMN)—is identified by the IMSI prefix, formed by combining the MCC and MNC.

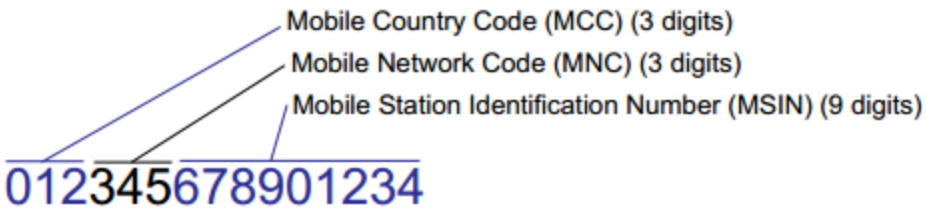
## IMSI on carrier networks

The International Mobile Subscriber Identity (IMSI) number is central to identifying users on a carrier network. It is a unique number that is assigned to a cell phone or mobile device to identify it on the GSM, UMTS, or LTE network.

Typical the IMSI number is stored on the SIM card of the mobile device and is sent to the network as required.

An IMSI number is 15 digits long, and includes the Mobile Country Code (MCC), Mobile Network Code (MNC), and Mobile Station Identification Number (MSIN).

**IMSI codes**




The Home Network Identity (HNI) is made up of the MCC and MNC. The HNI is used to fully identify a user's home network. This is important because some large countries have more than one country code for a single carrier. For example a customer with a mobile carrier on the East Coast of the United States would have a different MCC than a customer on the West Coast with the same carrier because even through the MNC would be the same the MCC would be different — the United States uses MCCs 310 to 316 due to its size.

If an IMSI number is not from the local carrier's network, IMSI analysis is performed to resolve the number into a Global Title which is used to access the user's information remotely on their home carrier's network for things like billing and international roaming.

## Adding basic filters

Use the following command to add a basic filter (or IMSI filter) to a GTP profile:

```
config firewall gtp
   edit <name>
```

```
set imsi-filter {disable | enable}
set default-imsi-action {allow | deny}
   config imsi
      edit <id>
         set mcc-mnc <mcc-mnc-name>
         set msisdn-prefix <prefix>
         set apnmember <apn-name>
         set action {allow | deny}
         set mode {ms | net | vrf}
      end
```

Set `default-imsi-action` to `allow` to allow traffic, then use `config imsi` to create IMSI filters to filter the allowed traffic. Set `default-imsi-action` to `deny` to block all traffic and then use `config imsi` to create IMSI filters that match the traffic to be allowed.

`mcc-mnc` optionally create a Mobile Country Code (MCC) and Mobile Network Code (MNC) to filter on. Together these numbers uniquely identify the carrier and network of the GGSN/PGW being used.

`msisidn-prefix` optionally create an MSISDN prefix to filter on.

`apnmember` optionally select one or more APNs and APN groups. To create APNs and APN groups, see APN filtering on page 37.

`mode` select one or more of the following modes. By default, all three modes are selected. The mode indicates where the APN originated and whether the Home Location Register (HLR) or Home Subscriber Server (HSS) has verified the user subscription.

- `ms` MS-provided APN, subscription not verified, indicates that the mobile station (MS) provided the APN and that the HLR/HSS did not verify the user's subscription to the network.
- `net` Network-provided APN, subscription not verified, indicates that the network provided a default APN because the MS did not specify one, and that the HLR/HSS did not verify the user's subscription to the network.
- `sub` MS or Network-provided APN, subscription verified, indicates that the MS or the network provided the APN and that the HLR/HSS verified the user's subscription to the network.

## Adding basic filters from the GUI

From the GUI:

1. Go to **Security Profiles > GTP Profiles**.
2. Add or edit a GTP profile and select **Basic Filtering**.
3. Set the **Default Action**.
4. Select **Create New** to add a basic filter.
5. Optionally select an **APN**. You can also create a new APN.
6. Optionally add an **MCC-MNC**.
7. Select the **Mode**.
8. Optionally add an **MSISDN**.
9. Set the **Action** to **Allow** or **Deny**.

# GTPv0/v1 policy filtering

GTPv0/v1 policy filtering (called Advanced filtering on the GTP profile GUI) supports filtering GTPv0/v1 traffic based on RAT, RAI, ULI, APN restriction, and IMEI-SV to block specific harmful GPRS traffic and GPRS roaming traffic. The following table shows some of the GTP context requests and responses that are supported.

| | GTP Create PDP Context Request | GTP Create PDP Context Response | GTP Update PDP Context Request | GTP Update PDP Context Response |
|---|---|---|---|---|
| **APN** | yes | yes | - | |
| **APN Restriction** | yes | - | - | yes |
| **IMEI-SV** | yes | - | - | - |
| **IMSI** | yes | - | yes | - |
| **RAI** | yes | - | yes | - |
| **RAT** | yes | - | yes | - |
| **ULI** | yes | - | yes | - |

## Adding GTPv0/v1 policy filters to a GTP profile

Use the following command to add an GTPv0/v1 policy filter to a GTP profile:

```
config firewall gtp
   edit <name>
      set default-policy-action {allow | deny}
         config policy
            edit <id>
               set apnmember <apn-name>
               set messages {create-req create-res update-req update-res}
               set apn-sel-mode {ms net vrf}
               set max-apn-restriction {all public-1 public-2 private-1 private-2}
               set imsi-prefix <prefix>
               set msisdn-prefix <prefix>
               set rat-type {any utran geran wlan gan hspa eutran virtual nbiot}
               set imei <imei-pattern>
               set action {allow | deny}
               set rai <rai-pattern>
               set uli <uli-pattern>
            end
```

Set `default-policy-action` to `allow` to allow traffic, then use `config policy` to create GTPv0/v1 policy filters to filter the allowed GTPv0/v1 traffic. Set `default-policy-action` to `deny` to block all traffic and then use `config policy` to create GTPv0/v1policy filters that match the GTPv0/v1f traffic to be allowed.

The `default-policy-action` setting applies to both GTPv0/v1 and GTPv2 policy filters. GTPv2 policy filtering is only active if the `policy-filter` option is enabled.

If you do not want your GTP profile to filter both GTPv0/v1 and GTPv2 traffic, you should disable the `policy-filter` option. If you enable the `policy-filter` option and set `default-policy-action` to `deny` and don't add a GTPv2 policy filter to your GTP profile, the GTP profile will block all GTPv2 traffic accepted by the firewall policy that the GTP profile is added to.

You can include the `*` wildcard character when adding IMEI, RAI, and ULI patterns. See the individual descriptions below for details.

`apnmember <apn-name>` add an APN or APN group to the policy filter.

`messages {create-req create-res update-req update-res}` select the content messages that a filter will match. Select one or more of the available options. Different policy options are available depending on the `messages` setting.

- `create-req` filter PDP context requests (the default). All policy filter options are available.
- `create-res` filter PDP context responses. Only the `max-apn-restriction` and `action` policy filter options are available.
- `update-req` filter update PDP context requests. Only the `imsi-prefix`, `rat-type`, `action`, `rai`, and `uli` policy filter options are available.
- `update-res` filter update PDP context responses. Only the `max-apn-restriction` and `action` policy filter options are available.

`apn-sel-mode {ms net vrf}` by default, all three modes are selected and this cannot be changed.

- `ms` MS-provided APN, subscription not verified, indicates that the mobile station (MS) provided the APN and that the HLR/HSS did not verify the user's subscription to the network.
- `net` Network-provided APN, subscription not verified, indicates that the network provided a default APN because the MS did not specify one, and that the HLR/HSS did not verify the user's subscription to the network.
- `sub` MS or Network-provided APN, subscription verified, indicates that the MS or the network provided the APN and that the HLR/HSS verified the user's subscription to the network.

`max-apn-restriction {all public-1 public-2 private-1 private-2}` select one or more of the following APN restrictions. For information about APN restrictions, see the GTPv1 spec 3GPP TS 29.060, section 7.7.49 APN Restriction.

- `all` (the default) match all APNs, no restrictions
- `public-1` match the Public-1 APN used on your network, for example MMS.
- `public-2` match your Public-2 APN used on your network, for example the internet.
- `private-1` match your Private-1 APN used on your network, for example Corporate users who use MMS.
- `private-2` match your Private-2 APN used on your network, for example Corporate users who do not use MMS.

`imsi-prefix` add an IMSI prefix.

`msisdn-prefix` add an MSISDN prefix.

`rat-type` select the Radio Access Technology (RAT) type as any combination of the following (some RAT types are GTPv1 specific). These fields control how a user accesses the carrier's network:

- `any` any RAT
- `utran` UTRAN
- `geran` GERAN

- `wlan` WLAN
- `gan` GAN
- `hspa` HSPA
- `eutran` EUTRAN
- `virtual` Virtual
- `nbiot` NB-IoT

`imei <imei-pattern>` add a single IMEI or an IMEI pattern that includes the `*` wildcard character to match multiple IMEIs. The IMEI uniquely identifies mobile hardware, and can be used to block stolen equipment.

A single IMEI must be in three parts separated by a decimal point in the format: `<8-digits>.<6-digits>.<1-or-2-digits>`. For example: 35349006.987300.1.

IMEI patterns must include the three decimal points. In each part of the IMEI pattern the `*` cannot be followed by a number. The following are some examples of valid IMEI patterns:

```
35349006.*.*
*.987*.1
*.*.*
```

`action {allow | deny}` allow (the default) or deny traffic matching this policy filter.

`rai <rai-pattern>` add a routing area identity (RAI) or an RAI pattern with the format `<MCC>.<MNC>.<LAC>.<RAC>`. The RAI must use the following number of digits (`d`) and hexadecimal numbers (`x`): `<ddd>.<dd>.<xxxx>.<xx>`. Example RAIs: `456.45.0c0c.0c` and `123.12.abab.0F`.

You can use the `*` wildcard to create RAI patterns that match more than one RAIs, for example: `456.45.0c0c.*`.

There is only one SGSN per routing area on a carrier network. This is often used with a ULI to locate a user geographically on a carrier network.

`uli` <uli-pattern> a user location identifier (ULI) or ULI pattern. The pattern can use one of the following formats:

A CGI ULI is prefixed with a 0 and uses the following format: `0:<MCC>.<MNC>.<LAC>.<CI>`.

A SAI ULI is prefixed with a 1 and uses the following format: `1:<MCC>.<MNC>.<LAC>.<SAC>`.

Both ULI types use the following number of digits (`d`) and hexadecimal numbers (`x`): `<ddd>.<dd>.<xxxx>.<xxxx>`.

Example CGI ULI: `0:465.23.0c0c.1f1f`. Example SAI ULI: `1:189.23.1a2c.3d4f`.

You can also use the `*` wildcard to create ULI patterns that match multiple ULIs. ULI patterns must include all of the required decimal points. In each part of the pattern, the `*` cannot be followed by a number. Example SAI ULI pattern: 1:189.23.1a2*.3d4f.

Often the ULI is used with the RAI to locate a user geographically on a carrier's network.

## GTPv0v1 policy filtering from the GUI

1. To create a new policy filter in a GTP profile, open **Advanced Filtering** and select **Create New**.
2. Select the PDP content **Messages** this advanced filter will match.

| | |
|---|---|
| **Create Request** | Filter PDP context requests. |
| **Create Response** | Filter PDP context responses. |

| | |
|---|---|
| **Update Request** | Filter update PDP context requests. |
| **Update Response** | Filter update PDP context responses. |

3. Select the APN Mode
4. Select the **APN restriction**:
   - All
   - Public-1
   - Public-2
   - Private-1
   - Private-2
5. Optionally add an **IMSI**.
6. Optionally add an **MSISDN**.
7. Optionally select the **RAT Type** as any combination of the following. Some RAT types are GTPv1 specific.
   - any
   - WiFi
   - eutran
   - UTRAN
   - GAN
   - virtual
   - GERAN
   - HSPA
   - nbiot
8. Optionally add a **ULI** pattern.
9. Optionally add a **RAI** pattern.
10. Optionally add an **IMEI** pattern.
11. Set the **Action** to **Allow** or **Deny**.
12. Select **OK** to save the filter.

## About patterns

When adding a rule, use the following formats:

- Prefix, for example, range 31* for MCC matches MCC from 310 to 319.
- Range, for example, range 310-319 for MCC matches MCC from 310 to 319.
- Mobile Country Code (MCC) consists of three digits. The MCC identifies the country of domicile of the mobile subscriber.
- Mobile Network Code (MNC) consists of two or three digits for GSM/UMTS applications. The MNC identifies the home PLMN of the mobile subscriber. The length of the MNC (two or three digits) depends on the value of the MCC. Best practices dictate not to mix two and three digit MNC codes within a single MCC area.
- Location Area Code (LAC) is a fixed length code (of 2 octets) identifying a location area within a PLMN. This part of the location area identification can be coded using a full hexadecimal representation except for the following reserved hexadecimal values: 0000 and FFFE. These reserved values are used in some special cases when no valid LAI exists in the MS (see 3GPP TS 24.008, 3GPP TS 31.102 and 3GPP TS 51.011).
- Routing Area Code (RAC) of a fixed length code (of 1 octet) identifies a routing area within a location.
- CI or SAC of a fixed length of 2 octets can be coded using a full hexadecimal expression.

- Type Allocation Code (TAC) has a length of 8 digits.
- Serial Number (SNR) is an individual serial number identifying each equipment within each TAC. SNR has a length of 6 digits.
- Software Version Number (SVN) identifies the software version number of the mobile equipment. SVN has a length of 2 digits.

### Radio Access Technology (RAT) type

The RAT type represents the radio technology used by the mobile device. This can be useful in determining what services or content can be sent to a specific mobile device. FortiOS Carrier supports:

- **UMTS Terrestrial Radio Access Network (UTRAN)**, commonly referred to as 3G, routes many types of traffic including IP traffic. This is one of the faster types.
- **GSM EDGE Radio Access Network (GERAN)** is a key part of the GSM network which routes both phone calls and data.
- **Wireless LAN (WLAN)** is used but not as widely as the other types. It is possible for the mobile device to move from one WLAN to another such as from an internal WLAN to a commercial hot spot.
- **Generic Access Network (GAN)** can also be called unlicensed mobile access (UMA). It routes voice, data, and SIP over IP networks. GAN is commonly used for mobile devices that have a dual-mode and can hand-off between GSM and WLANs.
- **High Speed Packet Access (HSPA)** includes two other protocols High Speed Downlink and Uplink Packet Access protocols (HSDPA and HSUPA respectively). It improves on the older WCDMA protocols by better using the radio bandwidth between the mobile device and the radio tower. This results in an increased data transfer rate for the user.

## GTPv2 policy filtering

GTPv2 policy filtering supports filtering GTPv2 traffic based on RAT, RAI, ULI, APN restriction, and IMEI-SV to block specific harmful GPRS traffic and GPRS roaming traffic.

### Adding GTPv2 policy filters to a GTP profile

Use the following command to add a GTPv2 policy filter to a GTP profile:

```
config firewall gtp
   edit <name>
      set policy-filter enable
      set default-policy-action {allow | deny}
      config policy-v2
         edit <id>
            set apnmember <apn-name>
            set messages {create-ses-req create-sess-res modify-bearer-req modify-bearer-res}
            set apn-sel-mode {ms net vrf}
            set max-apn-restriction {all public-1 public-2 private-1 private-2}
            set imsi-prefix <prefix>
            set msisdn-prefix <prefix>
            set rat-type {any utran geran wlan gan hspa eutran virtual nbiot item nr}
            set mei <mei-pattern>
            set action {allow | deny}
```

```
        set uli <cgi-uli-pattern> <sai-uli-pattern> <rai-uli-pattern> <rai-uli-pattern>
             <ecgi-uli-pattern> <lai-uli-pattern>
    end
```

You must enable `policy-filter` to enable GTPv2 policy filtering.

Set `default-policy-action` to `allow` to allow traffic, then use `config policy-v2` to create policy filters to filter the allowed traffic. Set `default-policy-action` to `deny` to block all traffic and then use `config policy-v2` to create policy filters that match the traffic to be allowed.

The `default-policy-action` setting applies to both GTPv0/v1 and GTPv2 policy filters.

If you set `default-policy-action` to `deny` and don't add a GTPv0/v1 policy filter to your GTP profile, the GTP profile will block all GTPv0/v1 traffic accepted by the firewall policy that the GTP profile is added to.

You can include the `*` wildcard character when adding MEI and ULI patterns. See the individual descriptions below for details.

`apnmember <apn-name>` add an APN or APN group to the policy filter.

`messages {create-ses-req create-sess-res modify-bearer-req modify-bearer-res}` select the content messages that the filter will match. Select one or more of the available options. Different policy filter options are available depending on the `messages` setting.

- `create-sess-req` create session request (the default). If you just select this message, all policy filter options are available.
- `create-sess-res` create session response. Only the `max-apn-restriction` and `action` policy filter options are available.
- `modify-bearer-req` modify bearer request. Only the `rat-type`, `action`, and `uli` policy filter options are available.
- `modify-bearer-res` modify bearer response. Only the `max-apn-restriction` and `action` policy filter options are available.

`apn-sel-mode {ms net vrf}` by default, all three modes are selected and this cannot be changed.

- `ms` MS-provided APN, subscription not verified, indicates that the mobile station (MS) provided the APN and that the HSS did not verify the user's subscription to the network.
- `net` Network-provided APN, subscription not verified, indicates that the network provided a default APN because the MS did not specify one, and that the HSS did not verify the user's subscription to the network.
- `sub` MS or Network-provided APN, subscription verified, indicates that the MS or the network provided the APN and that the HSS verified the user's subscription to the network.

`max-apn-restriction {all public-1 public-2 private-1 private-2}` select one or more of the following APN restrictions. For information about APN restrictions, see the GTPv2 spec 3GPP TS 29.274 V15.9.0, subsection 8.57 APN Restriction.

- `all` (the default) match all APNs with no restrictions.
- `public-1` match the Public-1 APN used on your network, for example MMS.
- `public-2` match your Public-2 APN used on your network, for example the internet.
- `private-1` match your Private-1 APN used on your network, for example Corporate users who use MMS.
- `private-2` match your Private-2 APN used on your network, for example Corporate users who do not use MMS.

`imsi-prefix <prefix>` add an IMSI prefix.

`msisdn-prefix <prefix>` add an MSISDN prefix.

`rat-type {any utran geran wlan gan hspa eutran virtual nbiot item nr}` set the RAT Type as any combination of the following:

- `any` any RAT (the default)
- `utran` UTRAN
- `geran` GERAN
- `wlan` WLAN
- `gan` GAN
- `hspa` HSPA
- `eutran` EUTRAN
- `virtual` Virtual
- `nbiot` NB-IoT
- `item` LTE-M
- `nr` NR

`mei <mei-pattern>` add a single MEI or an MEI pattern that includes the `*` wildcard character to match multiple MEIs. The MEI uniquely identifies mobile hardware, and can be used to block stolen equipment.

A single MEI must be in three parts separated by a decimal point in the format: `<8-digits>.<6-digits>.<1-or-2-digits>`. For example: 35349006.987300.1.

In each part of the MEI pattern the `*` cannot be followed by a number. The following are some examples of valid MEI patterns:

```
35349006.*.*
*.987*.1
*.*.*
```

`action {allow | deny}` allow (the default) or deny traffic matching this policy filter.

`uli <cgi-uli-pattern> <sal-uli-pattern> <rai-uli-pattern> <rai-uli-pattern> <ecgi-uli-pattern> <lai-uli-pattern>` add up to six different types of GTPv2 universal location information (ULI) patterns, separated by a space.

All of the ULI patterns have the format `<MCC>.<MNC>.<ID>.<[ID2]>`. `MCC` and `MNC` are decimal numbers of two or three digits (`d`). `ID` and `ID2` are hexadecimal numbers of four digits (`x`).

- `<cgi-uli-pattern>` a CGI ULI with the format `<ddd>.<dd[d]>.<xxxx>.<xxxx>`. Example CGI ULI: `123.12.0a0a.0F0F`.
- `<sai-uli-pattern>` is an SAI ULI with the format `<ddd>.<dd[d]>.<xxxx>.<xxxx>`. Example SAI ULI: `523.235.0b0a.0E0F`.
- `<rai-uli-pattern>` is a Routing Area Identity (RAI) ULI with the format `<ddd>.<dd[d]>.<xxxx>.<xx>`. Example RAI ULI: `456.45.0c0c.0c`.
- `<tai-uli-pattern>` is a Tracking Area Identity (TAI) ULI with the format `<ddd>.<dd[d]>.<xxxx>`. Example TAI ULI: `505.02.d008`.
- `<ecgi-uli-pattern>` is an E-UTRAN Cell Global Identifier (ECGI) ULI with the format `<ddd><dd[d]>.<xxxxxxx>`. Example ECGI ULI: `505.02.d008123`.
- `<lai-uli-pattern>` is a Location Area Identifier (LAI) ULI with the format `<ddd>.<dd[d]>.<xxxx>`. Example LAI ULI: `345.08.d009`.

Example syntax that includes all of the ULIs:

```
set uli 123.12.0a0a.0F0F 456.45.0b0b.0E0E 456.45.0c0c.0c 505.02.d008 505.02.d008123
     505.02.d009
```

If you do not need to include all six ULIs, you can enter a subset and use `0` as a placeholder for missing ULIs. You do not need to add trailing zeros. For example, if you only need to include a CGI and a SAI ULI, you can just enter the two ULIs as follows.

```
set uli 123.12.0a0a.0F0F 123.12.0a0a.0F0F
```

If you need to include a RAI and ECGI ULI, use 0s for the missing ULIs as follows:

```
set uli 0 0 456.45.0c0c.0c 0 505.02.d008123
```

You can also use the `*` wildcard to create ULI patterns that match multiple ULIs. ULI patterns must include all of the required decimal points. In each part of the pattern the `*` cannot be followed by a number.

Example CGI ULI pattern: `123.*.0a0a.0F0F`.

Example LAI ULI pattern: `345.08.d00*`.

# IE removal

In some roaming scenarios, FortiOS Carrier can be installed on the border of the PLMN and the IPX/GRX. In this configuration, FortiOS Carrier supports information element (IE) removal policies to remove any combination of R6 IEs (RAT, RAI, ULI, IMEI-SV and APN restrictions) prior to forwarding the messages to the HGGSN (proxy mode).

You can use the following command to enable IE removal and add IE removal policies to a GTP profile:

```
config firewall gtp
   edit <name>
      set ie-remover enable
         config ie-remove-policy
            edit <id>
               set sgsn-addr <ipv4-firewall-address>
               set sgsn-addr6 <ipv6-firewall-address>
               set remove-ies {apn-restriction rat-type rai uli imei}
            end
```

`sgsn-addr` select an IPv4 firewall address or address group to match the SGSNs or SGW addresses in the traffic for which to remove IEs. The default is `all`.

`sgsn-addr6` select an IPv6 firewall address or address group to match the SGSNs or SGW addresses in the traffic for which to remove IEs. The default is `all`.

`remove-ies` select one or more of the following IEs to be removed: `apn-restriction rat-type rai uli imei`. All of the IE types are selected by default.

From the GUI:

1. To create a new IE removal policy in a GTP profile, open **IE removal policy** and select **Create New**.
2. Select an **SGSN address** from the list of firewall addresses and address groups.
3. Select one or more of the following **IEs to be removed**.
   - APN
   - ULI
   - RAT Type
   - IMEI
   - RAI
4. Select **OK** to save the IE removal policy.

# IE validation

You can use the following command to add IE validation to a GTP profile. You can use IE validation to validate different types of content or messages in GTP traffic.

```
config firewall gtp
   edit <name>
      config ie-validation
         set imsi {disable | enable}
         set rai {disable | enable}
         set reordering-required {disable | enable}
         set ms-validated {disable | enable}
         set selection-mode {disable | enable}
         set nsapi {disable | enable}
         set charging-ID {disable | enable}
         set end-user-addr {disable | enable}
         set mm-context {disable | enable}
         set pdp-context {disable | enable}
         set gsn-addr {disable | enable}
         set msisdn {disable | enable}
         set qos-profile {disable | enable}
         set apn-restriction {disable | enable}
         set rat-type {disable | enable}
         set uli {disable | enable}
         set ms-tzone {disable | enable}
         set imei {disable | enable}
         set charging-gateway-addr {disable | enable}
      end
```

# Encapsulated IP traffic filtering

Encapsulated traffic on the GPRS network can come in a number of forms as it includes traffic that is “wrapped up” in another protocol. This detail is important for firewalls because it requires “unwrapping” to properly scan the data inside. If encapsulated packets are treated as regular packets, that inside layer will never be scanned and may allow malicious data into your network.

Generally there are a very limited number of IP addresses that are allowed to encapsulate GPRS traffic. For example GTP tunnels are a valid type of encapsulation when used properly. This is the GTP tunnel which uses the Gp or Gn interfaces between SGSNs and GGSNs or S5/S8 between SGWs and PGWs. However, a GTP tunnel within a GTP tunnel is not accessible — FortiOS Carrier will either block or forward the traffic, but is not able to open it for inspection.

You can use encapsulated IP traffic filtering (also just called IP filtering) to filter GTP sessions based on information contained in the data stream to control data flows within your infrastructure. You can configure IP filtering rules to filter encapsulated IP traffic from mobile stations according to source and destination IP addresses.

You can use the following command to enable encapsulated IP traffic filtering and add IP traffic filtering policies to a GTP profile:

```
config firewall gtp
   edit <name>
      set ip-filter enable
      set default-ip-action allow
         config ip-policy
```

```
edit <id>
   set srcaddr <address>
   set dstaddr <address>
   set srcaddr6 <address>
   set dstaddr6 <address>
   set action {deny | allow}
end
```

`ip-filter` enable or disable encapsulated IP traffic filtering. Disabled by default.

`default-ip-action` select `allow` (the default) to allow all sessions except those blocked by individual IP filters. Select `deny` to block all sessions except those allowed by individual IP filters.

`srcaddr`, `dstaddr`, `srcaddr6`, and `dstaddr6` select IPv4 and IPv6 firewall addresses or address groups to match the source and destination addresses of the traffic to be allowed or denied according to the `action`. You must select an address for each option. Select `all` to match all addresses. Select `none` to match no addresses. For example, if you want to create a filter that only filters IPv4 addresses, for `srcaddr6`, and `dstaddr6` select `none`.

`action` select whether to allow or deny traffic that matches the source and destination addresses. The default is `allow`.

From the GUI:

1. To create a new encapsulated IP traffic filter in a GTP profile, open **Encapsulated IP traffic filtering** and select **Create New**.
2. Select a **Source** firewall address or address group.
3. Select a **Destination** firewall address or address group.
4. Set Action to **Allow** or **Deny** encapsulated traffic between the source and destination addresses.
5. Select **OK** to save the filter.

## When to use encapsulated IP traffic filtering

The following are the typical cases that need encapsulated IP traffic filtering:

### Mobile station IP pools

In a well-designed network, best practices dictate that the mobile station address pool is to be completely separate from the GPRS network infrastructure range of addresses. Encapsulated IP packets originating from a mobile station will not contain source or destination addresses that fall within the address range of GPRS infrastructures. In addition, traffic originating from the users handset will not have destination/source IP addresses that fall within any Network Management System (NMS) or Charging Gateway (CG) networks.

### Communication between mobile stations

Mobile stations on the same GPRS network are not able to communicate with other mobile stations. Best practices dictate that packets containing both source and destination addresses within the mobile station's range of addresses are to be dropped.

### Direct mobile device or internet attacks

It may be possible for attackers to wrap attack traffic in GTP protocols and submit the resulting GTP traffic directly to a GPRS network element from their mobile stations or a node on the Internet. It is possible that the receiving SGSN or GGSN would then strip off the GTP header and attempt to route the underlying attack. This underlying attack could have any destination address and would probably have a source address spoofed as if it were valid from that PLMN.

You cannot add an IE removal policy when you are creating a new profile.

### Relayed network attacks

Depending on the destination the attack could be directly routed, such as to another node of the PLMN, or re wrapped in GTP for transmission to any destination on the Internet outside the PLMN depending on the routing table of the GSN enlisted as the unwitting relay.

The relayed attack could have any source or destination addresses and could be any of numerous IP network attacks, such as an attack to hijack a PDP context, or a direct attack against a management interface of a GSN or other device within the PLMN. Best practices dictate that any IP traffic originating on the Internet or from an MS with a destination address within the PLMN is to be filtered.

## Encapsulated non-IP end user traffic filtering

Much of the traffic on the GPRS network is in the form of IP traffic. However some parts of the network do not use IP based addressing,

Depending on the installed environment, it may be beneficial to detect GTP packets that encapsulate non-IP based protocols. You can configure FortiOS Carrier to permit a list of acceptable protocols, with all other protocols denied.

The encoded protocol is determined in the PDP Type Organization and PDP Type Number fields within the End User Address Information Element. The PDP Type Organization is a 4-bit field that determines if the protocol is part of the ETSI or IETF organizations. Values are zero and one, respectively. The PDP Type field is one byte long. Both GTP specifications list only PPP, with a PDP Type value of one, as a valid ETSI protocol. PDP Types for the IETF values are determined in the “Assigned PPP DLL Protocol Numbers” sections of RFC1700. The PDP types are compressed, meaning that the most significant byte is skipped, limiting the protocols listed from 0x00 to 0xFF.

You can use the following command to enable IP traffic filtering and add IP traffic filtering policies to a GTP profile:

```
config firewall gtp
   edit <name>
      set noip-filter enable
      set default-noip-action allow
         config noip-policy
            edit <id>
               set type {etsi | ietf}
               set start <protocl-number>
               set end <protocl-number>
               set action {allow | deny}
            end
```

`noip-filter` enable or disable non-IP end user traffic filtering. Disabled by default.

`default-noip-action` select `allow` (the default) to allow all sessions except those blocked by individual non-IP filters. Select `deny` to block all non-IP sessions except those allowed by individual filters.

`start` and `end` are used to select an IP protocol number range. The range can be from 0 to 255.

Select a start and end protocol from the list of protocols in RFC 1700. Allowed range includes 0 to 255 (0x00 to 0xff). Some common protocols include:

- 33 (0x0021) Internet Protocol
- 35 (0x0023) OSI Network Layer
- 63 (0x003f) NETBIOS Framing
- 65 (0x0041) Cisco Systems
- 79 (0x004f) IP6 Header Compression
- 83 (0x0053) Encryption

`action` select whether to allow or deny traffic that matches the `type` and IP protocol range. The default is `allow`.

From the GUI

1. To create a new non-IP end user traffic filtering, edit a GTP profile and open **Encapsulated non-IP traffic filtering**.
2. Set the **Default action** to **Allow** or **Deny**.
3. Select **Create New** to add a filter.
4. Set the **Type** to **ETSI** or **IETF**.
5. Enter the **Start** and **End protocol** numbers to define a protocol number range.
   Select a start and end protocol from the list of protocols in RFC 1700. Allowed range includes 0 to 255 (0x00 to 0xff). Some common protocols include:
   - 33 (0x0021) Internet Protocol
   - 35 (0x0023) OSI Network Layer
   - 63 (0x003f) NETBIOS Framing
   - 65 (0x0041) Cisco Systems
   - 79 (0x004f) IP6 Header Compression
   - 83 (0x0053) Encryption
6. Set Action to **Allow** or **Deny** encapsulated non-IP end user traffic based on the selected type and protocol range.
7. Select **OK** to save the filter.

# GTP protocol anomaly detection

The FortiOS Carrier firewall detects and optionally drops protocol anomalies according to GTP standards and specific tunnel states. Protocol anomaly attacks involve malformed or corrupt packets that typically fall outside of protocol specifications. These packets are not seen on a production network. Protocol anomaly attacks exploit poor programming practices when decoding packets, and are typically used to maliciously impair system performance or elevate privileges.

FortiOS Carrier also detects IP address spoofing inside GTP data channel.

By default, any GTP profile blocks traffic when the following GTP anomalies are detected:

- Invalid Reserved Field
- Reserved IE

- Miss Mandatory IE
- Out of State Message
- Out of State IE
- Spoofed Source Address

GTP protocol anomaly attacks involve malformed or corrupt packets that typically fall outside of the protocol specifications. If one of these anomalies is detected, the affected packet is blocked.

In a GTP profile, you can use the following options to deny or allow these anomalies. All are set to deny by default:

```
config firewall gtp
  edit <name>
    set invalid-reserved-field {allow | deny}
    set reserved-ie {allow | deny}
    set miss-must-ie {allow | deny}
    set out-of-state-message {allow | deny}
    set out-of-state-ie {allow | deny}
    set spoof-src-addr {allow | deny}
  end
```

| Anomaly | Description |
|---|---|
| `invalid-reserved-field` | On the GUI: **Invalid Reserved Field**. GTP version 0 (GSM 09.60) headers specify a number of fields that are marked as Spare and contain all ones (1). GTP packets that have different values in these fields are flagged as anomalies. GTP version 1 (GSM 29.060) makes better use of the header space and only has one, 1-bit, reserved field. In the first octet of the GTP version1 header, bit 4 is set to zero. |
| `reserved-ie` | On the GUI: **Reserved IE**. Both versions of GTP allow up to 255 different Information Elements (IE). However, a number of Information Elements values are undefined or reserved. Packets with reserved or undefined values will be filtered. |
| `miss-mandatory-ie` | On the GUI: **Miss Mandatory IE**. GTP packets with missing mandatory Information Elements (IE) will not be passed to the GGSN/PGW. |
| `out-of-state-message` | On the GUI: **Out of State Message**. The GTP protocol requires a certain level of state to be kept by both the GGSN and SGSN or the SGW and PGW. Some message types can only be sent when in a specific GTP state. Packets that do not make sense in the current state are filtered or rejected<br><br>Both versions of GTP allow up to 255 different message types. However, a number of message type values are undefined or reserved.<br><br>Best practices dictate that packets with reserved or undefined values will be filtered. |
| `out-of-state-ie` | On the GUI: **Out of State IE**. GTP Packets with out of order Information Elements are discarded. |
| `spoofed-source-addr` | On the GUI: **Spoofed Source Address**. The End User Address Information Element in the PDP Context Create & Response messages or in SGW and PGW sessions contains the address that the mobile station (MS) will use on the remote |

| Anomaly | Description |
| --- | --- |
| | network. If the MS does not have an address, the SGSN will set the End User Address field to zero when sending the initial PDP Context Create or Create Session Request message. The PDP Context Response packet or create session response packet from the GGSN will then contain an address to be assigned to the MS. In environments where static addresses are allowed, the MS will relay its address to the SGSN, which will include the address in the PDP Context Create or Create Session Request Message. If this option is set to deny, as the MS address is negotiated, any packets originating from the MS that contain a different source address are detected and dropped. |

## More about protocol anomaly detection

When anomalies do happen, it is possible for the anomaly to interrupt network traffic or consume network resources — if precautions are not taken. Anomalies can be generated by accident or maliciously, but both methods can have the same results — degrading the performance of the carrier network, or worse.

The following are some examples:

- The GTP header specifies the length of the packet excluding the mandatory GTP header. In GTP version 0 (GSM 09.60), the mandatory GTP header size is 20 bytes, whereas GTP version 1 (GSM 29.060) specifies that the minimum length of the GTP header is 8 bytes. The GTP packet is composed of the header, followed by Information Elements typically presented in a Type-Length-Value format. It is possible for an attacker to create a GTP packet with a GTP header field length that is incompatible with the length of the necessary information elements.
- The same concepts are true for GTP version 2 headers even though there are different fields in them.
- It is similarly possible for an attacker to create a packet with an invalid IE length. Invalid lengths may cause protocol stacks to allocate incorrect amounts of memory, and thereby cause crashes or buffer overflows.

By default, the FortiOS Carrier firewall detects these problems, as well as other protocol anomalies, and drops the packets. All protocol anomaly options are set to **Deny** by default. However, you can change the policy to allow them.

# Anti-overbilling

Overbilling can occur when a subscriber returns their IP address to the IP pool. Before the billing server closes it, the subscriber's session is still open and vulnerable. If an attacker takes control of the subscriber's IP address, the attacker can send or receive data and the subscriber will be billed for the traffic.

Overbilling can also occur when an available IP address is reassigned to a new mobile station (MS). Subsequent traffic by the previous MS may be forwarded to the new MS. The new MS would then be billed for traffic it did not initiate.

## Anti-overbilling with FortiOS Carrier

FortiOS Carrier can be configured to assist with anti-overbilling measures. These measures ensure that the customer is only billed for the connection time and data that they actually use.

Anti-overbilling involves:

- Configuring the overbilling settings in the GTP profile to notify the 2G or 3G Gi firewall or the 4G SGi firewall when a GTP tunnel is deleted
- FortiOS Carrier cleaning up any still running sessions when the Gi or SGi firewall receives a notification from the Gn/Gp/S5/S8 firewall about a GTP tunnel being deleted. This way, the Gi or SGi firewall prevents overbilling by blocking traffic initiated by other users.

## Setting up an interface to be the Gi or SGi gatekeeper

Use the following command to configure the port5 interface to be the Gi or SGi gatekeeper interface. This is the interface that FortiOS Carrier uses to communicate with the Gi or SGi firewall:

```
config system interface
   edit port5
      set gi-gk enable
   end
```

## Setting up Gi or SGi gatekeeper settings

Use the following command to configure anti-overbilling Gi or SGi gatekeeper settings:

```
config global
   config system gi-gk
      set context <context-id>
      set port <port-number>
   end
```

`context` the context ID of the network. This ID must match the ID entered on the Gi or SGi firewall. The default is 696.

`port` the port number used by the Gi or SGi firewall for anti-overbilling communication. The range is 0 to 65535. The default port is 21123.

From the GUI, go to **System > Settings > Gi Gatekeeper Settings** and configure the **Context ID** and **Port**.

## GTP profile anti-overbilling configuration

Use the following command to configure GTP anti-overbilling for traffic accepted by a GTP profile:

```
config firewall gtp
   edit <name>
      set addr-notify <ip-address>
      set port-notify <port-number>
      set interface-notify <interface-name>
      set context-id <context-id>
   end
```

`add-notify` the IP address of your Gi or SGi firewall.

`port-notify` the port number used by the Gi or SGi firewall for anti-overbilling communication. The range is 0 to 65535. The default port is 21123.

`interface-notify` select the interface through with FortiOS Carrier communicates with the Gi or SGi firewall.

`context-id` the context ID of the network. This ID must match the ID entered on the Gi or SGi firewall. The default is 696.

From the GUI:

1. To add anti-overbilling to a GTP profile, open **Anti-Overbilling**.
2. Add your network's **Gi Firewall IP Address** and the **Port** number that it uses (default 21123).
3. Select the **Interface** through which FortiOS Carrier communicates with the Gi firewall.
4. Enter your network's **Security Context ID** (default 696). This ID must match the ID entered on the server Gi firewall.

# Adding IE allow lists to GTP profiles

You can add an IE allow list to a GTP profile to allow GTP packets that contain out of state IEs in selected message types. Normally messages with out-of-state IEs would be blocked. But it you want to be able to allow some out-of-state IEs, you can add them to an IE allow list that contains pairs of allowed out-of-state IEs and message types. Then you can add this allow list to a GTP profile.

You can use the following command to create IE allow lists:

```
config gtp ie-white-list
   edit <ie-allow-list-name>
      config entries
         edit <index>
            set message <id>
            set ie <id>
         next
         edit <index>
            set message <id>
            set ie <id>
         end
```

You can use the following command to apply an IE allow list to GTPv0/v1 or GTPv2 traffic accepted by GTP profile:

```
config firewall gtp
   edit <name>
      set ie-white-list-v0v1 <ie-allow-list-name>
      set ie-white-list-v2 <ie-allow-list-name>
   end
```

# Logging

Use the following options to configure logging for a GTP profile.

```
config firewall gtp
   edit <name>
      set forwarded-log {disable | enable}
      set denied-log {disable | enable}
      set rate-limited-log {disable | enable}
      set state-invalid-log {disable | enable}
      set tunnel-limit-log {disable | enable}
      set extension-log {disable | enable}
      set traffic-count-log {disable | enable}
      set log-freq <frequency>
      set gtpu-forwarded-log {disable | enable}
      set gtpu-denied-log {disable | enable}
```

```
    set gtpu-log-freq <frequency>
    set log-gtpu-limit <limit>
    set log-imsi-prefix <prefix>
    set log-msisdn-prefix <prefix>
  end
```

GTP logs are a subtype of the event logs. You can view GTP logs by going to **Log & Report > GTP**.

From the GUI to configure logging in a GTP profile, open **Logging**.

| Option | Description |
|---|---|
| `forwarded-log` | GUI Forwarded Log. Enable to log forwarded GTP packets. Forwarded packets are allowed by the GTP profile. |
| `denied-log` | GUI Denied Log. Enable to log GTP packets denied or blocked by the GTP profile. |
| `rate-limited-log` | GUI Rate Limited Log. Enable to log rate-limited GTP packets. Rate limited packets have been dropped because they exceed the maximum rate limit of the destination GSN. |
| `state-invalid-log` | GUI State Invalid Log. Enable to log invalid GTP packets that have failed stateful inspection. |
| `tunnel-limit-log` | GUI Tunnel Limit Log. Enable to log packets dropped because the maximum limit of GTP tunnels for the destination GSN is reached. |
| `extension-log` | GUI Extension Log. Enable to log extended information about GTP packets. When enabled, this additional information will be included in log entries:<br>• IMSI<br>• MSISDN<br>• APN<br>• Selection Mode<br>• SGSN address for signaling<br>• SGSN address for user data<br>• SGW and PGW session information<br>• GGSN address for signaling<br>• GGSN address for user data |
| `traffic-count-log` | GUI Traffic count Log. Enable to log the total number of control and user data messages received from and forwarded to the GGSNs and SGSNs that the unit protects.<br>FortiOS Carrier can report the total number of user data and control messages received from and forwarded to the GGSNs and SGSNs it protects. Alternately, the total size of the user data and control messages can be reported in bytes. The unit differentiates between traffic carried by each GTP tunnel, and also between GTP-User and GTP-Control messages.<br>The number of messages or the number of bytes of data received from and forwarded to the SGSN or GGSN are totaled and logged if a tunnel is deleted.<br>When a tunnel is deleted, the log entry contains:<br>• Timestamp<br>• Interface name (if applicable)<br>• SGSN IP address |

| Option | Description |
|---|---|
| | • GGSN IP address<br>• SGW, PGW, and ePDG information<br>• TID<br>• Tunnel duration time in seconds<br>• Number of messages sent to the SGSN<br>• Number of messages sent to the GGSN |
| `log-freq` | GUI Log Frequency. The number of messages to drop between logged messages.<br>An overflow of log messages can sometimes occur when logging rate-limited GTP packets exceed their defined threshold. To conserve resources, you can specify that some log messages are dropped. For example, if you want only every twentieth message to be logged, set a log frequency of 20. This way, 20 messages are skipped and the next logged. Acceptable frequency values range from 0 to 2147483674. When set to '0', no messages are skipped. |
| `gtpu-forwarded-log` | GUI GTPU Forwarded Log: Enable to log forwarded GTPU packets. |
| `gtpu-denied-log` | GUI GTPU Denied Log. Enable to log GTPU packets denied or blocked by this GTP profile. |
| `gtpu-log-freq` | GUI GTPU Log Frequency. The number of messages to drop between logged GTPU messages. |
| `log-gtpu-limit` | The user data log limit in the range of 0 to 512 bytes. |
| `log-imsi-prefix` | Specify an IMSI prefix for selective logging |
| `log-msisdn-prefix` | Specify an MSISDN prefix for selective logging. |

## Log message content

Logging on the Carrier-enabled FortiGate unit is just like logging on any other FortiOS unit. The only difference with FortiOS Carrier is that there are a few additional events that you can log beyond the regular ones. These additional events are covered here.

To change FortiOS Carrier specific logging event settings, go to **Security Profiles > GTP Profile** and edit a GTP profile. Expand the **Log** section to change the settings. For detailed options, see Log options.

The following information is contained in each log entry:

| | |
|---|---|
| **Timestamp** | The time and date when the log entry was recorded |
| **Source IP address** | The sender's IP address. |
| **Destination IP address** | The receiver's IP address. The sender-receiver pair includes a mobile phone on the GPRS local network, and a device on a network external to the GPRS network, such as the Internet. |
| **Tunnel Identifier (TID)** | An identifier for the start and endpoints of a GTP tunnel. This information uniquely defines all tunnels. It is important for billing information based on the |

| | |
|---|---|
| **Tunnel Endpoint Identifier (TEID)** | length of time the tunnel was active and how much data passed over the tunnel. |
| **Message type** | For available message types, see Common message types on carrier networks. |
| **Packet status** | What action was performed on the packet. This field matches the logging options while you are configuring GTP logging. See Log message content on page 58.<br><br>The status can be one of forwarded, prohibited, state-invalid, rate-limited, or tunnel-limited |
| **Virtual domain ID or name** | Indicates the virtual domain (VDOM) that created the log message. If VDOMs are not enabled, this field will be `root`. |
| **Reason to be denied if applicable** | If the packet that generated this log entry was denied or blocked, this field will include what part of FortiOS denied or blocked that packet. Such as firewall, antivirus, webfilter, or spamfilter. |

An example of the above log message format is for a Tunnel deleted log entry. When a tunnel is deleted, the log entry contains the following information:

- Timestamp
- Interface name (if applicable)
- SGSN IP address (source IP)
- GGSN IP address (destination IP)
- Tunnel ID
- Tunnel duration time in seconds
- Number of messages sent to the SGSN
- Number of messages sent to the GGSN

# Improving NP6 GTP performance

FortiGate models with NP6 processors support improving FortiOS GTP performance by enabling the following option:

```
config system npu
   set gtp-support enable
   set gtp-enhanced-mode enable
end
```

`gtp-support` enable to offload GTP sessions to NP6 processors. This option is disabled by default.

`gtp-enhanced-mode` enable to improve performance of offloaded GTP sessions by configuring NP6 processors to set up independent Receive and Transmit queues for GTP-U processes. These queues and their associated resources are initialized when `gtp-enhanced-mode` is enabled. So after enabling or disabling `gtp-enhanced-mode`, you should restart your FortiGate to initialize the changes.

If you restore a configuration file, and if that restored configuration file has a different `gtp-enhanced-mode` setting, you should restart your FortiGate to initialize the changes.

Some FortiGate models running FortiOS Carrier include the following option that you can use to select the CPUs that can perform GTP-U packet inspection.

```
config system npu
   set gtp-enhanced-cpu-range {0 | 1 | 2}
end
```

Where:

`0` all CPUs will process GTP-U packets

`1` only primary CPUs will process GTP-U packets.

`2` only secondary CPUs will process GTP-U packets.

## Diagnose commands

**`diagnose npu np6 hbq-stats {all | np xx}`**

View the GTP-U packet counter for all of the NP6s or for a specific NP6 processor.

**`diagnose npu np6 hbq-stats-clear {all | np xx}`**

Clear the GTP-U packet counter for all of the NP6s or for a specific NP6 processor.

## Verifying that GTP enhanced-mode is enabled

Use `diagnose npu np6 hbq-stats all` to verify that `gtp-enhanced-mode` is enabled the output will be similar to below:

```
# diagnose npu np6 hbq-stats all
cpu_ 0:0
cpu_ 1:0
cpu_ 2:0
cpu_ 3:0
cpu_ 4:0
cpu_ 5:0
cpu_ 6:0
cpu_ 7:0
cpu_ 8:0
cpu_ 9:0
cpu_10:0
cpu_11:0
cpu_12:0
cpu_13:0
cpu_14:0
cpu_15:0
cpu_16:0
cpu_17:0
cpu_18:0
cpu_19:0
cpu_20:0
cpu_21:0
cpu_22:0
cpu_23:0
cpu_24:0
cpu_25:0
cpu_26:0
cpu_27:0
cpu_28:0
```

```
cpu_29:0
cpu_30:0
cpu_31:0
cpu_32:0
cpu_33:0
cpu_34:0
cpu_35:0
cpu_36:0
cpu_37:0
cpu_38:0
cpu_39:0
Total :0
```

# GTPv0/v1 message reference

FortiOS Carrier supports GTPv0/v1 message filtering by the type of message.

## Common message types on carrier networks

Carrier networks include many types of messages — some concern the network itself, others are content moving across the network, and still others deal with handshaking, billing, or other administration-based issues.

GTP contains two major parts GTP for the control plane (GTP-C) and GTP for user data tunneling (GTP-U). Outside of those areas there are only unknown message types.

## GTP-C messages

GTP-C contains the networking layer messages. These address routing, versioning, and other similar low level issues.

For GTPv0 and GTPv1, when a subscriber requests a Packet Data Protocol (PDP) context, the SGSN will send a create PDP context request GTP-C message to the GGSN giving details of the subscriber's request. The GGSN will then respond with a create PDP context response GTP-C message which will either give details of the PDP context actually activated or will indicate a failure and give a reason for that failure. This is a UDP message on port 2123.

GTP-C message types include Path Management Messages, Location Management Messages, and Mobility Management Messages.

## GTP-U messages

GTP-U is focused on user related issues including tunneling, and billing. GTP-U message types include MBMS messages, and GTP-U and Charging Management Messages.

## Unknown GTPv0v1 messages

Unknown messages are usually new messages that may be in use on your network but have only recently been added to GTPv0v1 by the 3GPP. These messages may be considered by the 3GPP as reserved or for future use. You can configure FortiOS Carrier GTPv0v1 message filtering to allow or deny unknown messages.

If you choose to deny unknown messages, you can create a list of unknown message types to allow if there are messages on your network unknown to FortiOS Carrier that you would like to allow. See GTPv0/v1 message filtering on page 28.

# Path management messages

Path management is used by one GSN to detect if another GSN is alive, or if it has restarted after a failure.

The path management procedure checks if a given GSN is alive or has been restarted after a failure. In case of SGSN restart, all MM and PDP contexts are deleted in the SGSN, since the associated data is stored in a volatile memory. In the case of GGSN restart, all PDP contexts are deleted in the GGSN.

| Message Type | Used by | Description |
|---|---|---|
| Echo Request (1)<br>Echo Response (2) | GTP-C, GTP-U, GTP' | Echo Request is sent on a path to another GSN to determine if the other node is alive. Echo Response is the reply. |
| Version Not Supported (3) | GTP-C, GTP-U, GTP' | There are multiple versions of GTP. Both devices communicating must use the same version of GTP, or this message will be the response. |
| Supported Extension Headers Notification (31) | | Extensions are optional parts that a device can choose to support or not. If a device includes these extensions, it must include headers for the extensions to sure ensure proper formatting. |

# Tunnel management messages

The tunnel management procedures are used to create, update, and delete GTP tunnels in order to route IP PDUs between an MS and an external PDN via the GSNs.

The PDP context contains the subscriber's session information when the subscriber has an active session. When a mobile wants to use GPRS, it must first attach and then activate a PDP context. This allocates a PDP context data structure in the SGSN that the subscriber is currently visiting and the GGSN serving the subscriber's access point.

Tunnel management procedures are defined to create, update, and delete tunnels within the GPRS backbone network. A GTP tunnel is used to deliver packets between an SGSN and a GGSN. A GTP tunnel is identified in each GSN node by a TEID, an IP address, and a UDP port number.

| Message Type | Used by | Description |
|---|---|---|
| Create PDP Context Request (16)<br>Create PDP Context Response (17) | GTP-C | Sent from an SGSN to a GGSN node as part of a GPRS PDP Context Activation procedure or the Network-Requested PDP Context Activation procedure. A valid request initiates the creation of a tunnel. |
| Update PDP Context Request (18)<br>Update PDP Context Response (19) | GTP-C | Used when PDP Context information changes, such as when a mobile device changes location. |
| Delete PDP Context Request (20)<br>Delete PDP Context Response | GTP-C | Used to terminate a PDP Context, and confirm the context has been deleted. |

| Message Type | Used by | Description |
|---|---|---|
| (21) | | |
| Create AA PDP Context Request/ Response | GTP-C | GTPv0, Sent as part of the GPRS Anonymous Access PDP Context Activation. It is used to create a tunnel between a context in the SGSN and a context in the GGSN. |
| Delete AA PDP Context Request (22)<br>Delete AA PD ContextResponse (23) | GTP-C | GTPv0, Sent as part of the GPRS PDP Anonymous Access Context Deactivation procedure to deactivate an activated PDP Context. It contains Cause and Private Extension Information Elements |
| Initiate PDP context activation request (22)<br>Initiate PDP context activation response (23) | GTP-C | GTPv1, The GGSN sends an Initiate PDP Context Activation Request message to the SGSN to initiate the Secondary PDP Context Activation Procedure for network requested bearer control. |
| Error Indication (26) | GTP-U | Sent to the GGSN when a tunnel PDU is received for the following conditions:<br><br>— No PDP context exists<br>— PDP context is inactive<br>— No MM context exists<br>— GGSN deletes its PDP context when the message is received. |
| PDU Notification Request (27)<br>PDU Notification Response (28)<br>PDU Notification Reject Request (29)<br>PDU Notification Reject Response (30) | GTP-C | When receiving a Tunneled PDU (T-PDU), the GGSN checks if a PDP context is established for the given PDP address. If no PDP context has been established, the GGSN may initiate the Network-requested PDP Context Activation procedure by sending a PDU Notification Request to the SGSN.<br><br>**Reject Request -** Sent when the PDP context requested by the GGSN cannot be established. |

# Mobility management messages

The MM procedures are used by a new SGSN in order to retrieve the IMSI and the authentication information or MM and PDP context information in an old SGSN. They are performed during the GPRS attach and the inter-SGSN routing update procedures.

The MM procedures are used between SGSNs at the GPRS-attach and inter-SGSN routing update procedures. An identity procedure has been defined to retrieve the IMSI and the authentication information in an old SGSN. This procedure may be performed at the GPRS attach. A recovery procedure enables information related to MM and PDP contexts in an old SGSN to be retrieved. This procedure is started by a new SGSN during an inter-SGSN RA update procedure.

| Message Type | Used By | Description |
|---|---|---|
| Identification Request (38)<br>Identification Response (39) | GTP-C | Sent by the new SGSN to the old SGSN to request the IMSI for a MS when a GPRS Attach is done with a P-TMSI and the MS has changed SGSNs since the GPRS Detach was done. |
| SGSN context Request (50)<br>SGSN context Response (51)<br>SGSN context Acknowledge (52) | GTP-C | Sent by the new SGSN to the old SGSN to request the MM and PDP Contexts for the MS. |
| Forward Relocation Request (53)<br>Forward Relocation Response (54)<br>Forward Relocation Complete (55)<br>Forward Relocation Complete Acknowledge (59) | GTP-C | Indicates mobile activation/deactivation within a Routing Area. This prevents paging of a mobile that is not active (visited VLR rejects calls from the HLR or applies Call Forwarding). Note that the mobile station does not maintain an attach/detach state.<br><br>SRNS contexts contain for each concerned RAB the sequence numbers of the GTP-PDUs next to be transmitted in uplink and downlink directions. |
| Relocation Cancel Request (56)<br>Relocation Cancel Response (57) | GTP-C | Send to cancel the relocation of a connection. |
| Forward SRNS Context (58)<br>Forward SRNS Context Acknowledge (60) | GTP-C | This procedure may be used to trigger the transfer of SRNS contexts from RNC to CN (PS domain) in case of inter system forward handover. |
| RAN Information Relay (70) | GTP-C | Forward the Routing Area Network (RAN) information.<br><br>A Routing Area (RA) is a subset of a GSM Location Area (LA). A RA is served by only one SGSN. Ensures that regular radio contact is maintained by the mobile |
| UE Registration Query Request (61)<br>UE Registration Query Response (62) | GTP-C | The request is sent by an SGSN to an MME to support CS/PS coordination for shared UTRAN and GERAN access. |

# Location management messages

The location-management procedure is performed during the network-requested PDP context activation procedure if the GGSN does not have an SS7 MAP interface (i.e., Gc interface). It is used to transfer location messages between the GGSN and a GTP-MAP protocol-converting GSN in the GPRS backbone network.

Location management subprocedures are used between a GGSN that does not support an SS7 MAP interface (i.e., Gc interface) and a GTP-MAP protocol-conversing GSN. This GSN supports both Gn and Gc interfaces and is able to perform a protocol conversing between GTP and MAP.

| Message Type | Used By | Description |
|---|---|---|
| Send Routing Information for GPRS Request (32)<br>Send Routing Information for GPRS Response (33) | GTP-C | Sent by the GGSN to obtain location information for the MS. This message type contains the IMSI of the MS and Private Extension.<br>Also written as Send Routeing Information for GPRS Request and Send Routeing Information for GPRS Response. |
| Failure Report Request (34)<br>Failure Report Response (35) | GTP-C | Sent by the GGSN to the HLR when a PDU reject message is received.<br><br>The GGSN requests the HLR to set the flag and add the GGSN to the list of nodes to report to when activity from the subscriber that owns the PDP address is detected.<br><br>The message contains the subscriber IMSI and Private Extension |
| Note MS GPRS Present Request (36)<br>Note MS GPRS Present Response (37) | GTP-C | When the HLR receives a message from a mobile with MDFG<br><br>set, it clears the MDFG and sends the Note MS Present message to all GGSNs in the subscriber's list.<br><br>This message type contains subscriber IMSI, GSN Address and Private Extension |

# GTPv0/v1 MBMS messages

Multimedia Broadcast and Multicast Services (MBMS) have recently begun to be offered over GSM and UMTS networks on UTRAN and GERAN radio access technologies. MBMS is mainly used for mobile TV, using up to four GSM timeslots for one MBMS connection. One MBMS packet flow is replicated by GGSN, SGSN and RNCs.

MBMS is split into the MBMS Bearer Service and the MBMS User Service. The MBMS User Service is basically the MBMS Service Layer and offers a Streaming- and a Download Delivery Method. The Streaming Delivery method can be used for continuous transmissions like Mobile TV services. The Download Method is intended for "Download and Play" services.

| Message Type | Used By | Description |
|---|---|---|
| MBMS Notification Request (96)<br>MBMS Notification Response (97)<br>MBMS Notification Reject Request (98)<br>MBMS Notification Reject Response (99) | GTP-C | Notification of the radio access devices. |
| Create MBMS Context Request (100) | GTP-C | Request to create an active MBMS context. The context will be pending until the response is received. |

| Message Type | Used By | Description |
|---|---|---|
| Create MBMS Context Response (101) | | Once active, the MBMS context allows the MS to receive data from a specific MBMS source |
| Update MBMS Context Request (102)<br>Update MBMS Context Response (103) | GTP-C | |
| Delete MBMS Context Request (104)<br>Delete MBMS Context Response (105) | GTP-C | Request to deactivate the MBMS context. When the response is received, the MBMS context will be inactive. |

# GTP-U and charging management messages

SGSNs and GGSNs listen for GTP-U messages on UDP port 2152.

GTP‘ (GTP prime) is used for billing messages. It uses the common GTP messages (GTP Version Not Supported, Echo Request and Echo Response) and adds additional messages related to billing procedures.

| Message Type | Used By | Description |
|---|---|---|
| G-PDU (255) | GTP-C, GTP-U | GPRS Packet data unit delivery message. |
| Node Alive Request (4)<br>Note Alive Response (5) | GTP-C, GTP-U | Used to inform rest of network when a node starts service. |
| Redirection Request (6)<br>Redirection Response (7) | GTP-C, GTP-U | Used to divert the flow of CDRs from the CDFs to another CGF when the sender is being removed, or they are used when the CGF has lost its connection to a downstream system. |
| Data Record Transfer Request (240)<br>Data Record Transfer Response (241) | GTP-C, GTP-U | Used to reliably transport CDRs from the point of generation (SGSN/GGSN) to non-volatile storage in the CGF |

# GTPv2 message reference

The GTPv2-C protocol creates, manages, and deletes SGW and PGW tunnels on Sx interfaces. GTPv2-C is used for the control plane path management, tunnel management and mobility management. It also controls forwarding relocation messages; SRNS context and creating forward tunnels during inter LTE handovers.

GTP-C message types include Path Management Messages, Location Management Messages, and Mobility Management Messages.

3GPP TS 29.274 lists and describes GTPv2 messages.

## Unknown GTPv2 messages

Unknown GTPv2 messages are usually new messages that may be in use on your network but have only recently been added to GTPv2 by the 3GPP. These messages may be considered by the 3GPP as reserved or for future use. You can configure FortiOS Carrier GTPv2 message filtering to allow or deny unknown messages.

If you choose to deny unknown messages, you can create a list of unknown message types to allow if there are messages on your network unknown to FortiOS Carrier that you would like to allow. For information about unknown message filtering, see GTPv2 message filtering on page 31.

## Path management message types

| Message type (value) | Description |
|---|---|
| Echo request (1) | Sent to a peer node on any GTPv2 interface to determine if the other node is alive and supports the same features as the sending node. |
| Echo response (2) | The reply to an echo request message. |
| Version not supported indication (3) | The message contains only the GTPv2 header and indicates the latest GTP version that the sending node supports. |

## Tunnel management message types

| Message type (value) | Description |
|---|---|
| Create session request (32) | GTPv2 sessions are started by a sender, such as an MME or PGW, sending a create session request over the S11 or S5/S8 interface to a receiver such as an SGW or PGW. The create session request message contains all of the IEs that the nodes require to establish the session. |

| Message type (value) | Description |
|---|---|
| Create session response (33) | Sent by a node in response to a create session request message. Create session responses include IEs required to establish the session. In addition, the create session response also indicates whether the sender can accept the request (for example, by including `Request accepted` or `Request accepted partially`) or not (for example, by including a description of the cause of the failure, for example, `Missing or unknown APN`). |
| Modify bearer request (34) | This multi-purpose message can be used for a number of purposes, for example:<br>• On the S5/S8 interface from the PGW to the SGW or on the S11 interface from the SGW to the MME during dedicated bearer activation.<br>• On the S5/S8 interface from the PGW to the SGW or on the S4 interface from the SGW to the SGSN during of secondary PDP context activation or network requested secondary PDP context activation.<br>• On the S2a interface from the PGW to the TWAN as part of dedicated bearer activation in WLAN on GTP S2a or on the S2b interface from the PGW to the ePDG during dedicated S2b bearer activation with GTP on S2b.<br>• On the S5/S8 or S2a/S2b interface from the PGW to the SGW or from the TWAN/ePDG or on the S11/S4 interface from the SGW to the MME/S4-SGSN during Network-initiated IP flow mobility or UE-initiated IP flow mobility. |
| Modify bearer response (35) | Sent by a node in response to a create bearer request message. Create bearer responses include IEs required to respond to the create bearer request. In addition, the create bearer response also indicates whether the sender can accept the request (for example, by including `Request accepted` or `Request accepted partially`) or not (for example, by including a description of the cause of the failure, for example, `Semantic error in the TFT operation`). |
| Bearer resource command (68) | Sent from an MME to a SGW and forwarded to the PGW during the UE requested bearer resource allocation or UE requested bearer resource modification. These operations are also used for dedicated bearer activation and deactivation.<br>Also sent on the S4 interface from a SGSN to a SGW and on the S5/S8 interface from a SGW to a PGW during MS-initiated PDP context modification, or secondary PDP context activation.<br>Also sent on the S11/S4 interface from an MME/S4-SGSN to a SGW and on the S5/S8 or S2a/S2b interface from a SGW or from a TWAN/ePDG to a PGW during UE-initiated IP flow mobility and UE requested IP flow mapping. |
| Bearer resource failure indication (69) | Sent by a node in response to a bearer resource command message to indicate a failure. Bearer resource failure indications include IEs required to respond to the command.The response also indicates the reason for the failure (for example, by including `Semantic errors in packet filtery`). |
| Modify bearer request (34) | This multi-purpose is sent as part of many processes to request changes or updates to processes or data. |

| Message type (value) | Description |
|---|---|
| Modify bearer response (35) | Sent by a node in response to a modify bearer request command message to respond to the request. Modify bearer responses include IEs required to respond to the modify bearer request. In addition, the modify bearer response also indicates whether the sender can accept the request (for example, by including `Request accepted` or `Request accepted partially`) or not (for example, `Service not supported`). |
| Delete session request (36)<br>Delete bearer request (99) | Sent in many different instances to end sessions or delete bearer resources in response to errors or changes in status or because sessions have ended. |
| Delete session response (37)<br>Delete bearer response (100) | Sent by a node in response to a delete session request or delete bearer request command message to respond to the request. The response messages include IEs to acknowledge that the delete request has been responded to. |
| Downlink data notification (176)<br>Downlink data notification acknowledge (177)<br>Downlink data notification failure indication (70) | Sent by nodes to notify downstream nodes to expect downlink data. Receiving nodes can use downlink data notification acknowledge messages to indicate if the node can fail or succeed in responding to the request. The downlink data notification failure is sent if a node can respond to the initial request but a failure occurs during the downlink operation. |
| Delete indirect data forwarding tunnel request (168) | Sent on the S4/S11 interface by the SGSN/MME to the SGW to delete indirect forwarding tunnels in source SGW/Target SGWs. |
| Delete indirect data forwarding tunnel response (169) | Sent on the S4/S11 interface by SGWs to SGSNs/MMEs as part of a variety of processes such as S1-based handovers, UTRAN Iu mode to E-UTRAN Inter RAT handovers, and so on. |
| Modify bearer command (64)<br>Modify bearer failure indication (65) | Sent over the S11 interface from the MME to the SGW or over the S5/S8 interface from the SGW to the PGW during HSS initiated subscribed QoS modification, or when the SQCI flag or the PSCI flag is set to 1 in the context response message.<br>Also sent over the S4 interface by the SGSN to the SGW or over the S5/S8 interface from the SGW to the PGW during the HSS Initiated subscribed QoS modification procedure or when the SQCI flag or the PSCI flag is set to 1 in the context response message.<br>Also sent on the S2a/S2b interface from the TWAN/ePDG to the PGW as part of HSS initiated subscribed QoS modification.<br>The failure indication is sent back to the sender of the modify bearer command if the command fails. |
| Update bearer request (97) | Sent from the PGW to the SGW, TWAN/ePDG or from the SGW to the MME/S4-SGSN as part of a number of processes that update bearer QoS and other settings. |
| Update bearer response (98) | Sent in response to an update bearer request to verify whether the bearer has been successfully modified by the request or not. |
| Delete bearer command (66)<br>Delete bearer failure indication (67) | Sent over the S11 interface from the MME to the SGW and over the S5/S8 interface from the SGW to the PGW during of the eNodeB requested bearer release or MME-initiated dedicated bearer deactivation. |

| Message type (value) | Description |
|---|---|
| | Also sent over the S4 interface from the SGSN to the SGW and over the S5/S8 interface from the SGW to the PGW during MS and SGSN initiated bearer deactivation using S4.<br>The failure indication message is sent in response to the delete bearer command if the request fails, and includes information about the reason for the failure. |
| Create indirect data forwarding tunnel request (166) | Sent on the S11/S4 interface by the MME/SGSN to the SGW during the handover or TAU/RAU procedure with serving GW change and data forwarding |
| Create indirect data forwarding tunnel response (167) | Sent by the SGW to the MME/SGSN as a response to a create indirect data forwarding tunnel request message to indicate if the indirect data forwarding tunnel has been created in the SGW or not and why if not successful. |
| Release access bearers request (170) | Sent on the S11 interface from the MME to the SGW during S1 release and eNodeB initiated connection suspend.<br>Also sent on the S11 interface from the MME to the SGW as part of the establishment of S1-U bearer during data transport in control plane CIoT EPS optimization procedure.<br>Also sent on the S4 interface from the SGSN to the SGW as part of the RAB release using S4, Iu Release using S4, or READY to STANDBY transition within the network. |
| Release Access Bearers Response (171) | Sent in response to release access bearers requests. The response indicates if the request is successful or not. |
| Stop paging indication (73) | Sent over the S11/S4 interface from the SGW to the MME/SGSN as a part of a network triggered service request. |
| Modify access bearers request (211) | Sent from the MME to SGW if both the SGW and the MME support the MABR feature. An MME sends a modify access bearer request message on the S11 interface to an SGW as part of a number of different processes that modify bearers. |
| Modify access bearers response (171) | Sent in response to modify access bearers requests to indicate whether the request was successful or not. |
| Remote UE report notification (40) | Sent be from MME to SGW and from SGW to PGW to notify the SGW that at least one remote UE is newly connected to or disconnected from a ProSe UE-to-network relay. |
| Remote UE report acknowledge (41) | The response to a remote UE report notification to acknowledge the information related to the remote UE(s) is received. |

# Mobility management messages

| Message type (value) | Description |
|---|---|
| Forward relocation request (133) | Sent between various nodes, for example between source and target MMEs or SGSNs as part of various handover or relocation processes. |
| Forward relocation response (134) | Response to forward relocation requests to confirm that the relocation was successful or not. |
| Forward relocation complete notification (135) | Sent to the source MME/SGSN/AMF to indicate a handover was successful. |
| Forward relocation complete acknowledge (136) | Response to a forward relocation complete notification. |
| Context request (130) | Sent by the new MME/SGSN to the old MME/SGSN on S3/S16/S10 interface as a part of TAU/RAU procedure and UTRAN/GERAN to E-UTRAN/UTRAN (HSPA) SRVCC procedure to get the MM and EPS bearer contexts for the UE. |
| Context response (131) | Response to a context request message. |
| Context acknowledge (132) | Response to a context response message |
| Identification request (128) | Sent by a UE when it changes SGSN or MME. The request is sent to the UE's old SGSN/MME/AMF. |
| Identification response (129) | Sent by the old SGSN/MME/AMF to the new MME/SGSN/AMF in response to a identification request message. |
| Forward access context notification (137) | Forward new RNC contexts to the new target system. Sent by the old SGSN to the new SGSN over the S16 interface.\<br>Can also forward RNC/eNodeB contexts to the new target system. Sent from the old MME to the new MME over the S10 interface. |
| Forward access context notification acknowledge (138) | Sent to the old MME/SGSN as a response to Forward access context notification. |
| Detach notification (149) | Sent by various nodes as part of a detach procedure. |
| Detach acknowledge (150) | Response to a detach notification. |
| Change notification request (38) | Used for reporting of changes of UE presence in presence reporting areas or user CSG information change reporting. |
| Change notification response (39) | Response to a change notification request. Includes information about whether the change was successful or not. |
| Relocation cancel request (139) | Sent from the source MME/SGSN/AMF to the target MME/SGSN/AMF on S3/S10/S16/N26 interface during a handover or relocation cancel procedure. |
| Relocation cancel response (140) | Response to a relocation cancel request. Includes information about whether the cancel request was successful or not. |

| Message type (value) | Description |
|---|---|
| Configuration transfer tunnel (141) | Set up a tunnel to securely transfer configuration transfer messages between source and target MMEs or between MMEs and AMFs. |
| RAN information relay (152) | Transfer the RAN information received by an SGSN from BSS or RNS (or GERAN Iu mode) or by an MME from eNodeB. Also to transfer the RAN information between GERAN or GERAN Iu mode or UTRAN. |
| ISR status indication (157) | Sent on the S3 interface by the MME/SGSN to the ISR associated SGSN/MME to:<br>• Restore PDN connections after an SGW failure for UEs.<br>• Begin the HSS Based P-CSCF restoration procedure for 3GPP access (for both basic and PCO extension). |
| UE registration query request (158) | Supports CS/PS coordination for shared UTRAN and GERAN access. |
| UE registration query response (159) | Response to a UE registration query. Includes information about whether the query was successful or not. |

## Restoration and recovery message types

| Message type (value) | Description |
|---|---|
| PGW downlink notification (103) | Also called PGW downlink triggering notification. The PGW Downlink Triggering Notification is sent as part of the PGW triggered SGW restoration procedure if the MME/S4-SGSN, SGW and PGW support this optional feature. |
| PGW downlink acknowledge (104) | Also called PGW downlink triggering acknowledge. The PGW Downlink Triggering Acknowledge message is sent as a response to a PGW Downlink Triggering Notification message if the MME/S4-SGSN, SGW and PGW support the PGW triggered SGW restoration feature. |
| PGW restart notification (179) | If both the SGW and the MME/S4-SGSN support the PRN feature, a PGW Restart Notification is sent when the SGW detects that the peer PGW has restarted, and a PGW Restart Notification can also be sent when the SGW detects that the peer PGW has failed and not restarted. |
| PGW restart acknowledge (180) | The PGW Restart Notification Acknowledge is sent in response to a PGW restart notification. |

## CS Fallback and SRVCC related messages

| Message type (value) | Description |
|---|---|
| Suspend notification (162) | Sent as part of CS fallback processes to suspend a UE. After receiving a suspend notification message, the SGW/PGW marks all the non-GBR bearers as suspended status. |
| Suspend acknowledge (163) | Reply to a suspend notification to acknowledge the notification. |
| Resume notification (164) | Sent as part of a process to resume a suspended node or UE. |
| Resume acknowledge (165) | Reply to a resume notification to acknowledge the notification. |
| CS paging indication (151) | Sent on the S3 interface by the MME to the associated SGSN when ISR is activated as part of mobile terminated CS services. |
| Alert MME notification (153) | Sent on the S3 interface by the MME to the associated SGSN as part of an SGs Non-EPS alert procedure when ISR is activated. |
| Alert MME acknowledge (154) | Reply to an alert MME notification to acknowledge the notification. |
| UE activity notification (155) | Sent on the S3 interface from the SGSN to the associated MME as part of an SGs non-EPS alert when ISR is activated to indicate that activity from a UE has been detected. |
| UE activity acknowledge (156) | Reply to an UE activity notification to acknowledge the notification. |

## GTPv2 MBMS messages

| Message type (value) | Description |
|---|---|
| MBMS session start request (231) | The MBMS session start request message is sent on the Sm/Sn interface by the MBMS GW to the MME/SGSN when a new session is starting. |
| MBMS session start response (232) | The MBMS session start response message is sent as a response to the MBMS session start request message from the MME/SGSN to the MBMS GW. |
| MBMS session update request (233) | The MBMS session update request message is sent on the Sm/Sn interface by the MBMS GW to the MME/SGSN to update session status information. |
| MBMS session update response (234) | The MBMS session update response message is sent as a response to a MBMS session update request message. |
| MBMS session stop request (235) | The MBMS session stop request message is sent on the Sm/Sn interface by the MBMS GW to the MME/SGSN when an established session has been stopped. |
| MBMS session stop response (236) | The MBMS session stop response message is sent as a response to a MBMS session stop request message. |

# Non-3GPP access related messages

| Message type (value) | Description |
|---|---|
| Create forwarding tunnel request (160) | Sent by an MME to a serving GW when the MME configures resources for indirect data forwarding during active handover from E-UTRAN to CDMA 2000 HRPD access. |
| Create forwarding tunnel response (161) | Reply to a create forwarding tunnel request to respond the request. |
| Reserved for earlier version of the GTP specification (178). | This message type is for future use. |

# SCTP Concepts

SCTP is a connection-oriented transport protocol that overcomes some of the limitations of both TCP and UDP that prevent reliable transfer of data over IP-based networks (such as those used by telephony systems and carrier networks). The 'Stream' in SCTP refers to the sequence of user messages or packets that are considered at the same time to be individual objects and also treated as a whole by networked systems. SCTP is less vulnerable to congestion and flooding due to more advanced error handling and flood protection built into the protocol.

**SCTP features as compared to TCP and UDP**

| Feature | SCTP | TCP | UDP |
|---|---|---|---|
| State required at each endpoint | yes | yes | no |
| Reliable data transfer | yes | yes | no |
| Congestion control and avoidance | yes | yes | no |
| Message boundary conservation | yes | no | yes |
| Path MTU discovery and message fragmentation | yes | yes | no |
| Message bundling | yes | yes | no |
| Multi-homed hosts support | yes | no | no |
| Multi-stream support | yes | no | no |
| Unordered data delivery | yes | no | yes |
| Security cookie against SYN flood attack | yes | no | no |
| Built-in heartbeat (reachability check) | yes | no | N/A |

All of these features are built into the design of the Protocol, and the structure of SCTP packets and networks. The FortiGate unit interprets the traffic and provides the necessary support for maintenance and verification features, but the features are not FortiGate specific. These features are documented in greater detail below.

## SCTP firewall

Stream Control Transmission Protocol (SCTP) is part of the Transport Layer of the OSI Model just like TCP and UDP and provides some of the features of both of those protocols. It is message or datagram orientated like UDP but it also ensures reliable sequential transport of data with congestion control like TCP.

SCTP provides the following services:

- Acknowledged error-free non-duplicated transfer of user data
- Data fragmentation to conform to discovered path MTU size
- Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages

- Optional bundling of multiple user messages into a single SCTP packet
- Network-level fault tolerance through supporting of multi-homing at either or both ends of an association
- Congestion avoidance behavior and resistance to flooding and masquerade attacks

SCTP uses multi-streaming to transport its messages which means that there can be several independent streams of messages traveling in parallel between the points of the transmission. The data is sent out in larger chunks of data than is used by TCP just like UDP but the messages include a sequence number within each message in the same way that TCP does so that the data can be reassembled at the other end of the transmission in the correct sequence without the data having to arrive in the correct sequence.

SCTP is effective as the transport protocol for applications that require monitoring and session-loss detection. For such applications, the SCTP path and session failure detection mechanisms actively monitor the connectivity of the session. SCTP differs from TCP in having multi-homing capabilities at either or both ends and several streams within a connection, typically referred to as an association. A TCP stream represents a sequence of bytes; an SCTP stream represents a sequence of messages.

Some common applications of SCTP include supporting transmission of the following protocols over IP networks:

- SCTP is important in 3G and 4G/LTE networks (for example, HomeNodeB = FemtoCells)
- SS7 over IP (for example, for 3G mobile networks)
- SCTP is also defined and used for SIP over SCTP and H.248 over SCTP
- Transport of Public Switched Telephone Network (PSTN) signaling messages over IP networks.

SCTP is a much newer protocol. It was defined by the IETF Signaling Transport (SIGTRAN) working group in 2000. It was introduced by RFC 3286 and more fully defined by RFC 4960.

The FortiGate and FortiOS Carrier firewall can apply security policies to SCTP sessions in the same way as TCP and UDP sessions. You can create security policies that accept or deny SCTP traffic by setting the service to “ALL”. FortiOS does not include pre-defined SCTP services. To configure security policies for traffic with specific SCTP source or destination ports you must create custom firewall services for SCTP.

FortiOS and FortiOS Carrier routes SCTP traffic in the same way as TCP and UDP traffic. You can configure policy routes specifically for routing SCTP traffic by setting the protocol number to 132. SCTP policy routes can route SCTP traffic according to the destination port of the traffic if you add a port range to the policy route.

You can configure a FortiOS and FortiOS Carrier to perform stateful inspection of different types of SCTP traffic by creating custom SCTP services and defining the port numbers or port ranges used by those services. FortiOS and FortiOS Carrier supports SCTP over IPv4.

FortiOS and FortiOS Carrier perform the following checks on SCTP packets:

- Source and Destination Port and Verification Tag.
- Chunk Type, Chunk Flags and Chunk Length.
- Verify that association exists.
- Sequence of Chunk Types (INIT, INIT ACK, etc).
- Timer checking.
- Four way handshake checking.
- Heartbeat mechanism.
- Protection against INIT/ACK flood DoS attacks, and long-INIT flooding.
- Protection against association hijacking.

FortiOS also supports SCTP sessions over IPsec VPN tunnels, as well as full traffic and event logging for SCTP sessions.

Example firewall policy that can accept SCTP traffic:

```
config firewall policy
   edit <id>
      set name "sctp-example"
      set srcintf "port1"
      set dstintf "port2"
      set action accept
      set srcaddr "all"
      set dstaddr "all"
      set schedule "always"
      set service "ALL"
   end
```

## State required at each endpoint

Constant back and forth acknowledgment and content verification messages are sent between all SCTP peer endpoints, and all endpoints' state machine actions must be synchronized for traffic to flow.

## Reliable data transfer

SCTP places data and control information (for example, source, destination, verification) into separate messages, both sharing the same header in the same SCTP packet. This allows for constant verification of the contained data at both ends and along the path, preventing data loss or fragmentation. As well, data is not sent in an interruptible stream as in TCP.

## Congestion control and avoidance

Built-in, constantly updating path detection and monitoring automatically redirect packets along alternate paths in case of traffic congestion or inaccessible destinations.

## Message boundary conservation

SCTP is designed in such a way that no matter how messages are divided, redirected, or fragmented, the message boundaries will be maintained within the packets, and all messages cannot be appended without tripping verification mechanisms.

## Path MTU discovery and message fragmentation

SCTP is capable of Path Maximum Transmission Unit discovery, as outlined in RFC4821. Two specific alterations have been made to how SCTP handles MTU. First, that endpoints will have separate MTU estimates for each possible multi-homed endpoint. Second, that bundled message fragments (as explained below) will be directed based on MTU calculations, so that retransmissions (if necessary) will be sent without delay to alternate addresses.

## Message bundling

SCTP is a message-oriented protocol, which means that despite being a streaming data protocol, it transports a sequence of specific messages, rather than transporting a stream of bytes (like TCP). Since some data transmissions are small enough to not require a complete message's worth of content, so multiple pieces of content will be transmitted simultaneously within the messages.

## Multi-homed hosts support

SCTP supports multi-homing, which is a network structure in which one or multiple sources/destinations has more than one IP address. SCTP can adapt to multi-homing scenarios and redirect traffic to alternate IP addresses in case of failure.

## Multi-stream support

Due to the message bundling feature allowing for multiple pieces of content to be sent in messages at once, SCTP can 'multi-stream' content, by deliberately dividing it among messages at a fixed rate, so that multiple types of content (for example, both images and text) can be loaded at once, at the same pace.

## Unordered data delivery

With control messages in every packet to provide verification of any packet's data and its place in the stream, the data being transmitted can actually arrive in any order, and verify that all has arrived or that some is missing.

## Security cookie against SYN flood attack

Since every packet contains verification of its place in the stream, it makes it easy for the protocol to detect when redundant, corrupted or malicious packets flood the path, and they are automatically dropped when necessary.

# Built-in heartbeat (reachability check)

Endpoints automatically send specific control chunks among the other SCTP packet information to peer endpoints, to determine the reachability of the destination. Heartbeat acknowledgment packets are returned if the destination is available.

# MMS Configuration

Since MMS profiles can be used by more than one security policy, you can configure one profile for the traffic types handled by a set of security policies requiring identical protection levels and types, rather than repeatedly configuring those same profile settings for each individual security policy.

If the security policy requires authentication, do not select the MMS profile in the security policy. This type of profile is specific to the authenticating user group. For details on configuring the profile associated with the user group, see User Groups in the Authentication guide.

For example, while traffic between trusted and untrusted networks might need strict protection, traffic between trusted internal addresses might need moderate protection. To provide the different levels of protection, you might configure two separate protection profiles: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks.

Once you have configured the MMS profile, you can then apply the profile to MMS traffic by applying it to a security policy.

MMS profiles can contain settings relevant to many different services. Each security policy uses the subset of the MMS profile settings that apply to the sessions accepted by the security policy. In this way, you might define just one MMS profile that can be used by many security policies, each policy using a different or overlapping subset of the MMS profile.

MMS profiles contains options for each of the following types of configuration:

- MMS scanning
- MMS Bulk Email Filtering Detection
- MMS Address Translation
- MMS Notifications
- DLP Archive
- Logging

## MMS profile scanning options

This section describes the options available in MMS profiles to configure scanning options for each of the MMS protocols. The following MMS profile CLI options are described.

```
config firewall mms-profile
   edit <name>
      set comment <sting>
      set replacemsg-group
      set mmsbwordthreshold <threshold>
      set mm1comfortinterval <interval>
      set mm7comfortinterval <interval>
      set mm1comfortamount <amount>
      set mm7comfortamount <amount>
      set mm1-addr-hdr <string>
      set mm7-addr-hdr <string>
```

```
    set mm1-addr-source {cookie | http-header}
    set mm7-addr-source {cookie | http-header}
    set mm1-convert-hex {disable | enable}
    set mm7-convert-hex {disable | enable}
    set carrier-endpoint-prefix {disable | enable}
    set remove-blocked-const-length {disable | enable}
    set mm1 {avmonitor oversize scan bannedword chunkedbypass clientcomfort servercomfort
         carrier-endpoint-bwl remove-blocked mms-checksum}
    set mm1-retrieve-scan {disable | enable}
    set mm3 {avmonitor oversize scan bannedword fragmail splice carrier-endpoint-bwl
         remove-blocked mms-checksum}
    set mm4 {avmonitor oversize scan bannedword fragmail splice carrier-endpoint-bwl
         remove-blocked mms-checksum}
    set mm7 {avmonitor oversize scan bannedword chunkedbypass clientcomfort servercomfort
         carrier-endpoint-bwl remove-blocked mms-checksum}
    set mm1oversizelimit <limit>
    set mm3oversizelimit <limit>
    set mm4oversizelimit <limit>
    set mm7oversizelimit <limit>
    set mm1-retr-dupe {disable | enable}
    set carrierendpointbwltable <index>
    set avnotificationtable <index>
    set mms-checksum-table <index>
    set bwordtable <index>
end
```

The same MMS scanning options can be applied to each protocol except that:

- `chunkedbypass`, `clientcomfort`, and `servercomfort` can be applied to MM1 and MM7 only.
- `fragmail` and `splice` can be applied to MM3 and MM4 only.

| Option | Description |
|---|---|
| `avmonitor` | Record log messages when MMS scanning finds a virus, matches a file name, or matches content using any of the other MMS scanning options. Select this option to be able to report on viruses and other problems in MMS traffic without affecting users. |
| `oversize` | Block oversized files or emails in MMS traffic. If this option is not selected, oversize files are passed through without being scanned. Use `mm1oversizelimit <size>`, `mm3oversizelimit <size>`, `mm4oversizelimit <size>`, and `mm7oversizelimit <size>` to set the oversized file threshold in Kbytes. The range is 1 to 819200 Kbytes and the default is 10240 Kbytes. The oversize limit refers to the final size of the message, including attachments, after encoding by the client. Clients can use a variety of encoding types; some result in larger file sizes than the original attachment. As a result, a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the oversize threshold. |
| `scan` | Scan attachments in MMS traffic for viruses.Since MM1 and MM7 use HTTP, the oversize limits for HTTP and the HTTP antivirus port configuration also applies to MM1 and MM7 scanning.MM3 and MM4 use SMTP and the oversize limits for |

| Option | Description |
|---|---|
| | SMTP and the SMTP antivirus port configuration also applies to MM3 and MM4 scanning.You can enable or disable `mm1-retrieve-scan` (enabled by default) to enable or disable scanning MM1 retrieve configuration messages.You can enable `mm1-retr-dupe` (disabled by default) to prevent scanning of duplicate MM1 retrieval messages. Disabling `mm1-retr-dupe` can improve performance.Use the `avnotificationtable <index>` option to select an antivirus notification table. Use the `config antivirus notification` command to create an antivirus notification table. |
| `bannedword` | Filter messages based on matching the content of the message with the words or patterns in a selected web content filter list. Use `bwordtable <index>` to add a web content filter list to the MMS profile. Use the `config webfilter content` command to add a web content filter list. Use the `mmsbwordthreshold <number>` option to set the number of banned words that content blocking must find before FortiOS Carrier considers the content to have too many banned words. The rang is 0 to 2147483647 and the default is 10. |
| `chunkedbypass` | Pass chunked MM1 and MM7 massages. Chunked content cannot be scanned for viruses. If you do not select `chunkedbypass`, FortiOS Carrier blocks chunked MM1 and MM7 messages. Chunking is a mechanism in version 1.1 of HTTP that allows a web server to start sending chunks of dynamically generated output in response to a request before knowing the actual size of the content. |
| `fragmail` | Pass fragmented MM3 and MM4 messages. Fragmented messages cannot be scanned for viruses. If you do not select `fragmail`, FortiOS Carrier blocks fragmented MM3 and MM4 messages. |
| `{clientcomfort \| servercomfort}` | Enable client comforting and server comforting for MM1 and MM7 sessions. You can use client and server comforting to prevent client and server connection timeouts that can occur while waiting for FortiOS Carrier to buffer and scan large requests from slow servers or clients.Use `mm1comfortinterval <time>` and `mm7comfortinterval <time>` to control the time in seconds before client and server comforting starts after a download has begun, and the time between sending subsequent data. The range is 1 to 900 seconds and the default is 10 seconds.Use `mm1comfortamount <bytes>` and `mm7comfortamount <bytes>` to control the number of bytes sent by client or server comforting at each interval. The range is 1 to 65535 bytes and the default is 1 byte. |
| `carrier-endpoint-bwl` | Add carrier endpoint content filtering. Use `carrierendpointbwltable` to select a carrier endpoint content filter list to add to the MMS profile. Use the `config firewall carrier-endpoint-bwl` command to add carrier endpoint content filter lists. |
| `remove-blocked` | Remove content intercepted by MMS scanning options and replace it with the appropriate replacement message.Enable `remove-blocked-const-length` to preserve the message size when removing blocked content. Use this option if billing is affected by message size. |
| `mms-checksum` | Add MMS content checksums to an MMS profile. Use `mms-checksum-table` to select the MMS content checksum list to apply to the profile. Use the `config` |

| Option | Description |
|---|---|
| | `antivirus mms-checksum` command to add MMS checksums. Use the `config antivirus mms-checksum` to create checksum lists. |
| `replacemsg-group <index>` | Specify the replacement messages group to apply to traffic processed by this MMS profile. |
| `{mm1-addr-hdr \| mm7-addr-hdr} <string>` | Specify the MM1 or MM7 header field that this MMS profile looks in for user addresses. Use a text string to specify the field name. For both options, the default is `x-up-calling-line-id`. |
| `{mm1-addr-source \| mm7-addr-source} {cookie \| http-header}` | Specify whether the MMS profile finds MM1 and MM7 source addresses in the HTTP header (`http-header`) or from cookies (`cookie`). The default is `http-header`. |
| `{mm1-convert-hex \| mm7-convert-hex} {disable \| enable}` | Enable or disable converting MM1 or MM7 user addresses from hex strings to digital IP addresses. This option is disabled by default. |

# Logging

You can enable logging in an MMS profile to write event log messages when the MMS profile options that you have enabled perform an action. For example, if you enable MMS antivirus protection, you could also use the MMS profile logging options to write an event log message every time a virus is detected.

MMS profile logging options are:

```
config firewall mms-profile
  edit <name>
    set mms-carrier-endpoint-filter-log {disable | enable}
    set mms-antispam-mass-log {disable | enable}
    set mms-notification-log {disable | enable}
    set mms-checksum-log {disable | enable}
    set mms-av-virus-log {disable | enable}
    set mms-av-block-log {disable | enable}
    set mms-av-oversize-log {disable | enable}
    set mms-web-content-log {disable | enable}
  end
```

| Option | Description |
|---|---|
| `mms-carrier-endpoint-filter-log` | Enable to log MMS carrier endpoint filter events, such as MSISDN filtering. |
| `mms-antispam-mass-log` | Enable to log MMS Bulk AntiSpam events (called message floods). |
| `mms-notification-log` | Enable to log the number of MMS notification messages sent. |
| `mms-checksum-log` | Enable to log MMS content checksum activity. . |

| Option | Description |
|---|---|
| mms-av-virus-log | Enable to record a log message when this MMS profile detects a virus. |
| mms-av-block-log | Enable to record a log message when antivirus file filtering enabled in this MMS profile blocks a file. |
| mms-av-oversize-log | Enable to record a log message when this MMS profile encounters an oversized file or email message. |
| mms-web-content-log | Enable to log content blocking events. |

# Virus outbreak and external threat feeds

You can use the following command to add FortiGuard virus outbreak prevention and external threat feed protection to an MMS profile.

```
config firewall mms-profile
   edit profile-name
      config outbreak-prevention
         set ftgd-service {disable | enable}
         set external-blocklist {disable | enable}
      end
   end
```

Enabling `ftgd-service` allows you to apply the FortiGuard virus outbreak service to traffic processed by this MMS profile.

Enabling `external-blocklist` allows you to apply configured threat feeds to the traffic processed by this MMS profile. Configure threat feeds from the GUI by going to **Security Fabric > Fabric Connectors > Threat Feeds**. From the CLI you can configure threat feeds using the `config system external-resource` command. All configured threat feeds are applied to the traffic processed by the MMS profile.

# MMS bulk anti-spam detection options

You can use the `config flood` and `config dupe` sections of the `config firewall MMS-profile` command to configure bulk email filtering options to detect and filter MM1 and MM4 message floods and duplicate messages. You can configure three thresholds that define a flood of message activity and three thresholds that define excessive duplicate messages. The configuration of each threshold includes the response actions to follow when the threshold is reached.

The configurable thresholds for each of the flood and duplicate sensors and must be enabled in sequence. For example, you can enable Flood Threshold 1 and Flood Threshold 2, but you cannot disable Flood Threshold 1 and enable Flood Threshold 2. When each threshold is met, FortiOS Carrier performs the configured action for the specified duration.

You can also add MSISDNs to the bulk email filtering configuration and select a subset of the bulk email filtering options to apply to these individual MSISDNs.

## Message flood configuration

Use the following command to configure the first threshold for MM1 and MM4 message flood protection.

```
config firewall mms-profile
   edit <name>
      config flood {mm1| mm4}
         set status1 {disable | enable}
         set window1 <window>
         set limit1 <limit>
         set action1 {block archive log archive-first alert-notif}
         set block-time1 <time>
         set status2 {disable | enable}
         set window2 <window>
         set limit2 <limit>
         set action2 {block archive log archive-first alert-notif}
         set block-time2 <time>
         set status3 {disable | enable}
         set window3 <window>
         set limit3 <limit>
         set action3 {block archive log archive-first alert-notif}
         set block-time3 <time>
      end
```

| Option | Description |
|---|---|
| `status1`<br>`status2`<br>`status3` | Enable each option to apply an additional level of flood protection. |
| `window1`<br>`window2`<br>`window3` | Enter the period of time during which a message flood will be detected if `limit1` is exceeded. The message flood window can be 1 to 2880 minutes (48 hours).<br>• The default value of window1 is 60.<br>• The default value of window2 is 70.<br>• The default value of window1 is 80. |
| `limit1`<br>`limit2`<br>`limit3` | Enter the number of messages which signifies a message flood if exceeded within the `window1` time. |
| `action1`<br>`action2`<br>`action3` | Select one or more actions to perform when a message flood is detected:<br>`block` Block user messages.<br>`archive` Content archive user messages.<br>`log` Log user messages.<br>`archive-first` Content archive only first message.<br>`alert-notif` Send an alert notification message. |
| `block-time1`<br>`block-time2`<br>`block-time3` | Enter the amount of time during which FortiOS performs the `action` after a message flood is detected. |

## Duplicate message detection

Use the following command to configure the first threshold for MM1 and MM4 duplicate message protection.

```
config firewall mms-profile
   edit <name>
      config dupe {mm1 | mm4}
         set status1 {disable | enable}
         set window1 <window>
         set limit1 <limit>
         set action1 {block archive log archive-first alert-notif}
         set block-time1 <time>
         set status2 {disable | enable}
         set window2 <window>
         set limit2 <limit>
         set action2 {block archive log archive-first alert-notif}
         set block-time2 <time>
         set status3 {disable | enable}
         set window3 <window>
         set limit3 <limit>
         set action3 {block archive log archive-first alert-notif}
         set block-time3 <time>
      end
```

The second and third thresholds have the same options except the keywords end with a 2 and 3 (for example, `status2`, `status3`, and so on).

| | |
|---|---|
| `status1`<br>`status2`<br>`status3` | Enable each option to apply an additional level of duplicate message protection. |
| `enable1`<br>`enable2`<br>`enable3` | Enable the selected duplicate message threshold and to make the rest of the options available for configuration. |
| `window1`<br>`window2`<br>`window3` | Enter the period of time during which excessive message duplicates will be detected if the Duplicate message Limit it exceeded. The duplicate message window can be 1 to 2880 minutes (48 hours).<br>• The default value of window1 is 60.<br>• The default value of window2 is 70.<br>• The default value of window1 is 80. |
| `limit1`<br>`limit2`<br>`limit3` | Enter the number of messages which signifies excessive message duplicates if exceeded within the Duplicate Message Window. |
| `action1`<br>`action2`<br>`action3` | Select one or more actions that FortiOS is to perform when excessive message duplication is detected:<br>`block` Block user messages.<br>`archive` Content archive user messages.<br>`log` Log user messages.<br>`archive-first` Content archive only first message.<br>`alert-notif` Send an alert notification message. |
| `block-time1` | Enter the amount of time during which FortiOS performs the `action` excessive message duplication is detected. |

## Flood and duplicate message thresholds for individual MSISDNs

You can use the following command to send flood and duplication message threshold notifications to specific MSISDNs. You can use this option as another way to notify administrators of message floods or excessive numbers of duplication messages by sending text messages to their MSISDNs.

```
config firewall mms-profile
   edit <name>
   config notif-msisdn
      edit <msisdn>
         set threshold {dupe-thresh-1 dupe-thresh-2 dupe-thresh-3 flood-thresh-1 flood-
              thresh-2 flood-thresh-3}
      end
```

| | |
|---|---|
| <msisdn> | The recipient MSISDN. |
| flood-thresh-1 | Send flood threshold 1 notifications to the recipient MSISDN. |
| flood-thresh-2 | Send flood threshold 2 notifications to the recipient MSISDN. |
| flood-thresh-3 | Send flood threshold 3 notifications to the recipient MSISDN. |
| dupe-thresh-1 | Send duplicate threshold 1 notifications to the recipient MSISDN. |
| dupe-thresh-2 | Send duplicate threshold 2 notifications to the recipient MSISDN. |
| dupe-thresh-3 | Send duplicate threshold 3 notifications to the recipient MSISDN. |

# MM1 and MM7 address translation options

The sender’s carrier endpoint is used to provide logging and reporting details to the mobile operator and to identify the sender of infected content.

When MMS messages are transmitted, the **From** field may or may not contain the sender's address. When the address is not included, the sender information will not be present in the logs and FortiOS will not be able to notify the user if the message is blocked unless the sender's address is made available elsewhere in the request.

FortiOS can extract the sender's address from an extended HTTP header field in the HTTP request. This field must be added to the HTTP request before it is received by FortiOS. If this field is present, it will be used instead of the sender's address in the MMS message for logging and notification. If this header field is present when a message is retrieved, it will be used instead of the To address in the message. If this header field is not present, FortiOS uses the content of the To header field instead.

Alternatively, FortiOS can extract the sender’s address from a cookie.

You can configure MMS address translation to extract the sender’s carrier endpoint so that it can be added to log and notification messages. You can configure MMS address translation settings to extract carrier endpoints from HTTP header fields or from cookies. You can also configure MMS address translation to add an endpoint prefix to the extracted carrier endpoints.

```
config firewall mms profile
   edit <name>
      set mm1-addr-source
      set mm7-addr-source
      set mm1-addr-hdr
```

```
    set mm7-addr-hdr
    set mm1-convert-hex
    set mm7-convert-hex
    set carrier-endpoint-prefix
    set carrier-endpoint-prefix-string
    set carrier-endpoint-prefix-range-min
    set carrier-endpoint-prefix-range-max
end
```

| MMS Address Translation | |
|---|---|
| mm1-addr-source<br>mm7-addr-source | Extract the sender's address source from the HTTP Header Field (http-header) or a Cookie. |
| mm1-addr-hdr<br>mm7-addr-hdr | Enter the sender address identifier that includes the carrier endpoint. The default identifier is x-up-calling-line-id.<br><br>If the sender address source is http-header, the address and its identifier in the HTTP request header takes the format:<br><br><Sender Address Identifier>: <MSISDN_value><br><br>Where the <MSISDN_value> is the carrier endpoint. For example, the HTTP header might contain:<br><br>x-up-calling-line-id: 6044301297<br><br>where x-up-calling-line-id would be the Sender Address Identifier.<br><br>If the sender address source is cookie, the address and its identifier in the HTTP request header's cookie field takes the format of attribute-value pairs:<br><br>Cookie: id=<cookie-id>;<br><br><Sender Address Identifier>=<MSISDN Value><br><br>For example, the HTTP request headers might contain:<br><br>Cookie: id=0123jf!a;x-up-calling-line-id=6044301297<br><br>where x-up-calling-line-id would be the sender address identifier. |
| mm1-convert-hex<br>mm7-convert-hex | Enable to convert the sender address from ASCII to hexadecimal or from hexadecimal to ASCII. This is required by some applications. |
| carrier-endpoint-prefix | Enable to add the country code to the extracted carrier endpoint, such as the MSISDN, for logging and notification purposes. You can limit the number length for the test numbers used for internal monitoring without a country code. |
| carrier-endpoint-prefix-string | Enter a carrier endpoint prefix to be added to all carrier endpoints. Use the prefix to add extra information to the carrier endpoint in the log entry. |

| MMS Address Translation | |
|---|---|
| carrier-endpoint-prefix-range-min | Enter the minimum length of the country code information being added. If this and Maximum Length are set to zero (0), length is not limited. |
| carrier-endpoint-prefix-range-max | Enter the maximum length of the country code information being added. If this and Minimum Length are set to zero (0), length is not limited. |

# MMS Notifications

MMS notifications are messages that a unit sends when an MMS profile matches content in an MM1, MM3, MM4 or MM7 session. For example, the MMS profile detects a virus or uses content blocking to block a web page, text message or email. You can send notifications to the sender of the message using same protocol and the addressing headers in the original message. You can also configure MMS notifications to send notification messages to another destination (such as a system administrator) using the MM1, MM3, MM4 or MM7 protocol.

You need to enable one or more **Notification Types** or you can add an **Antivirus Notification List** to enable sending notifications,.

You can also use MMS notifications options to configure how often notifications are sent. The unit sends notification messages immediately for the first event, then at a configurable interval if events continue to occur. If the interval does not coincide with the window of time during which notices may be sent, the unit waits to send the notice in the next available window. Subsequent notices contain a count of the number of events that have occurred since the previous notification.

There are separate notifications for each notification type, including virus events. Virus event notifications include the virus name. Up to three viruses are tracked for each user at a time. If a fourth virus is found, one of the existing tracked viruses is removed from the list.

The notifications are MM1 `m-send-req` messages sent from the unit directly to the MMSC for delivery to the client. The host name of the MMSC, the URL to which `m-send-req` messages are sent, and the port must be specified.

```
config firewall mms-profile
   edit <name>
      set avnotificationtable
         config notification {mm1 | mm3 | mm4 | mm7)
            set <notification options>
         end
```

| MMS Notification | |
|---|---|
| avnotificationtable | Optionally select an antivirus notification list to select a list of virus names to send notifications for. The unit sends a notification message whenever a virus name or prefix in the antivirus notification list matches the name of a virus detected in a session scanned by the MMS protection profile. Select **Disabled** if you do not want to use a notification list.<br><br>Instead of selecting a notification list you can configure the **Virus ScanNotification Type** to send notifications for all viruses. |

| MMS Notification | |
|---|---|
| msg-protocol | Select the protocol used to send notification messages. You can use a different protocol to send the notification message than the protocol on which the violation was sent. The MMS Notifications options change depending on the message protocol that you select.<br><br>If you select a different message protocol, you must also enter the User Domain. If selecting MM7 you must also enter the Message Type. |
| detect-server | Select to use the information in the headers of the original message to set the address of the notification message. If you do not select this option, you can enter the required addressing information manually.<br><br>You cannot select **Detect Server Details** if you are sending notification messages using a different message protocol.<br><br>If you select **Detect Server Details**, you cannot change the **Port** where the notification is being sent. |
| mmsc-hostname | Enter the FQDN or the IP address of the server where the notifications will be sent. |
| mmsc-url | Enter the URL of the server. For example if the notification is going to www.example.com/home/alerts , the URL is /home/alerts.<br><br>This option is available only when **Message Protocol** is **mm1** or **mm7**. |
| mmsc-port | Enter the port number of the server.<br><br>You cannot change the ***Port*** if ***Detect Server Details*** is enabled. |

# Troubleshooting

This section offers troubleshooting options for Carrier-related issues.

## FortiOS Carrier diagnose commands

This section includes diagnose commands specific to FortiOS Carrier features such as GTP.

### GTP related diagnose commands

This CLI command allows you to gain information on GTP packets, logs, statistics, and other information.

```
diag firewall gtp <command>
```

| | |
|---|---|
| apn list <gtp_profile> | The APN list entries in the specified GTP profile |
| auth-ggsns show <gtp_profile> | The authorized GGSNs entries for the specified GTP profile. Any GGSNs not on this list will not be recognized. |
| auth-sgsns show <gtp_profile> | The authorized SGSNs list entries for the specified GTP profile. Any SGSNs not on this list will not be recognized. |
| handover-grp show <gtp_profile> | The handover group showing the range of allowed handover group IP addresses. The handover group acts like a list of allowed GTP addresses with a default deny at the end — if the GTP address is not on the list, it is denied. |
| ie-remove-policy list <gtp_profile> | List of IE policies in the IE removal policy for this GTP profile. The information displayed includes the message count for this policy, the length of the SGSN, the list of IEs, and list of SGSN IP addresses. |
| imsi list <gtp_profile> | IMSI filter entries for this GTP profile. The information displayed includes the message count for this filter, length of the IMSI, the length of the APN and IMSI, and of course the IMSI and APN values. |
| invalid-sgsns-to-log list <gtp_profile> | List of SGSNs that do not match the filter criteria. These SGSNs will be logged. |
| ip-policy list <gtp_profile> | List the IP policies including message count for each policy, the action to take, the source and destination IP addresses or ranges, and masks. |
| noip-policy list <gtp_profile> | List the non-IP policies including the message count, which mode, the action to take, and the start and end protocols to be used by decimal number. |
| path {list \| flush} | Select list or flush.<br><br>List the GTP related paths in FortiOS Carrier memory. |

| | |
|---|---|
| | Flush the GTP related paths from memory. |
| policy list <gtp_policy> | The GTP advanced filter policy information for this GTP profile. The information displayed for each entry includes a count for messages matching this filter, a hexadecimal mask of which message types to match, the associated flags, action to take on a match, APN selection mode, MSISDN, RAT types, RAI, ULI, and IMEI. |
| profile list | Displays information about the configured GTP profiles.<br><br>You will not be able to see the bulk of the information if you do not log the output to a file. |
| runtime-stat flush | Select to flush the GTP runtime statistics from memory. |
| stat | Display the GTP runtime statistics — details on current GTP activity. This information includes how many tunnels are active, how many GTP profiles exist, how many IMSI filter entries, how many APN filter entries, advanced policy filter entries, IE remove policy filter entries, IP policy filter entries, clashes, and dropped packets. |
| tunnel {list \| flush \| filter} | Select one of list or flush.<br><br>List lists all the GTP tunnels currently active.<br><br>Flush clears the list of active GTP tunnels. This does not clear the clash counter displayed in the `stat` command. |

# Diagnose firewall gtp tunnel list command

The `diagnose fiewall gtp tunnel list` command displays information about all of the active GTP tunnels, for example:

```
diagnose firewall gtp tunnel list
list gtp tunnels

-----------prof=S11u-profile_check_on_RAT=NBIOT ref=6 imsi=208930123000001
msisdn=012300000100000 mei=35349006.987300.1 ms_addr=10.45.0.194 s11_s4 1-----------
-----------index=00000062 life=1438(sec) idle=1438(sec) vd=0  ver=2-----------
c_pkt=2 c_bytes=384 u_pkt=0 u_bytes=0
downlink cfteid:
    addr=172.30.111.2 teid=0x00000001 role=control vd=0 intf_type=s11 mme gtp-c
uplink cfteid:
    addr=172.30.111.4 teid=0x000000c1 role=control vd=0 intf_type=s11/s4 sgw gtp-c
1/1 bearers:
    id=5 linked_id=0 type=regular dead=0 apn=internet selection=ms-or-net-provided-apn apn_
restriction=all user_addr=10.45.0.194 u_pkt=0 u_bytes=0
    2 fteids:
        addr=172.30.111.6 teid=0x00000182 role=data vd=0 intf_type=s1-u sgw gtp-u
        addr=172.30.111.7 teid=0x00000182 role=data vd=0 intf_type=s5/s8 pgw gtp-u
```

**Notes about the command output**

`Index=00000062` means 6x16 + 2 = 98 decimal as shown in GTP Log.

`downlink cfteid, addr=172.30.111.2` is the source of the GTP-C `create_session_request`. The field `inf_type=s11` indicates MME.

`uplink cfteid, addr=172.30.111.4` is the source of the GTP-C `create_session_response`. The field `intf_type=s11/s4` indicates SGW.

For the bearers, GTP-U traffic (information as received from the SGW in the `Create_Session_Response`) includes the following fields:

- `addr=172.30.111.6` GTP-U from eNodeB to SGW (S1-U).
- `addr=172.30.111.7` GTP-U from PGW to SGW (S5-U).

# Applying IPS signatures to IP packets within GTP-U tunnels

GTP-U (GTP user data tunneling) tunnels carry user data packets, signaling messages and error information. GTP-U uses UDP port 2152. Carrier-enabled FortiGate units can apply IPS intrusion protection and detection to GTP-U user data sessions.

To apply IPS to GTP-U user data sessions, add an IPS Sensor to a profile and add the profile to a security policy that accepts GTP-U tunnels. The security policy Service field must be set to GTP or ANY to accept GTP-U packets.

The Carrier-enabled FortiGate unit intercepts packets with destination port 2152, removes the GTP header and handles the packets as regular IP packets. Applying an IPS sensor to the IP packets, the Carrier-enabled FortiGate unit can log attacks and pass or drop packets depending on the configuration of the sensor.

If the packet is GTP-in-GTP, or a nested tunnel, the packets are passed or blocked without being inspected.

**To apply an IPS sensor to GTP-U tunnels**

1. Go to **Security Profiles > Intrusion Prevention** and select Create New (**+**) to add an IPS Sensor.
2. Configure the IPS Sensor to detect attacks and log, drop, or pass attack packets.
3. Go to **Policy & Objects > IPv4 Policy** and apply the IPS sensor to the security policy.
4. Go to **Policy & Objects > IPv4 Policy** and select Create New to add a security policy or select a security policy.
5. Configure the security policy to accept GTP traffic.
   In the security policy configure the source and destination settings to match the GTP traffic. Service to GTP or ANY so that the security policy accepts GTP traffic.
6. Select the GTP profile within the security policy.
7. Configure any other required security policy settings.
8. Select **OK** to save the security policy.

# GTP packets are not moving along your network

When GTP packets are not getting to their destination, this could be caused by any one of a number of issues. General troubleshooting principals apply here.

The following sections provide some suggestions on how to troubleshoot this issue:

- Attempt to identify the section of your network with the problem
- Ensure you have an APN configured
- Check the logs and adjust their settings if required
- Check the routing table
- Perform a sniffer trace
- Generate specific packets to test the network

## Attempt to identify the section of your network with the problem

The first step is to determine how widespread this problem is. Does it affect the whole GPRS network, or just one or two devices?

If the entire network is has this problem, the solution is likely a more general one such as ensuring the security policies allow GTP traffic to pass, the GTP profile specifies SSGNs and GSGNs, or ensuring the GTP general settings are not overly limiting.

If one part of the network is affected, the problem is more likely centered around configurations with those network devices specified such as the handover group, or authorized SGSNs/GGSNs. It is also possible that small portions of the network may have hardware related issues such as cabling or faulty hardware. This section does not address those issues, and assumes hardware is not the problem.

The handover group is a list of GTP addresses allowed to handle GTP messages. If a device's address is not on this list, it will be denied.

## Ensure you have an APN configured

When you configure your GTP profile, ensure you first configure the APN. Without it, there will be no flow of traffic. The APN is used in nearly all GTP communications and without it, the Carrier-enabled FortiGate unit doesn't have the information it needs.

## Check the logs and adjust their settings if required

During normal operation, the log settings will show any problems on the network but may not provide the level of details required to fully troubleshoot the problem. The reason for this is that the level of detail required for troubleshooting would quickly overwhelm the daily logs without any real benefit.

GTP related events in the event log will have message IDs in the range 41216 to 41222. For more information on GTP log messages, see the Log Message Reference. For more information on logging in general, see the Logging and Reporting guide.

Once there is a problem to troubleshoot, check the logs to trace the traffic patterns and narrow down the possible sources of the problem. There may be enough detail for you to locate and fix the problem without changing the log settings.

Remember to set any changes you made to the log settings back to their original values when you are done troubleshooting. Otherwise, the amount of detail will overwhelm your logging.

However, if more detail is required you can change settings such as:

- Lower the Log Frequency number in GTP Profiles so fewer or no log messages are dropped. This will allow a more accurate picture of everything happening on the network, where you may have had only a partial picture before.
- Ensure all the GTP log events are enabled to provide you with a complete picture.
- Ensure that all relevant event types are enabled under **Log & Report > Log Config > Log Settings.**

For more information on GTP related logging, see Logging events on the Carrier-enabled FortiGate unit.

General information to look for in the logs includes:

- Are all packets having problems or just certain types?
- Are all devices on the network having problem, or just certain devices?
- Is it just GTP traffic that is having problems or are all types of traffic having the same problem?

## Check the routing table

On any network, the routing table determines how packets reach their destination. This is also true on a carrier network.

If the Carrier-enabled FortiGate unit is running in NAT mode, verify that all desired routes are in the routing table — local subnets, default routes, specific static routes, and dynamic routing protocols. For complete information, it is best to check the routing table in the CLI. This method provides more complete information.

If VDOMs are enabled on your Carrier-enabled FortiGate unit, all routing related CLI commands must be performed within a VDOM and not in the global context.

**To check the routing table using the CLI**

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

S* 0.0.0.0/0 [10/0] via 192.168.183.254, port2
S 1.0.0.0/8 [10/0] via 192.168.183.254, port2
S 2.0.0.0/8 [10/0] via 192.168.183.254, port2
C 10.142.0.0/23 is directly connected, port3
B 10.160.0.0/23 [20/0] via 10.142.0.74, port3, 2d18h02m
C 192.168.182.0/23 is directly connected, port2
```

Examining an entry from the routing table above:

```
B 10.160.0.0/23 [20/0] via 10.142.0.74, port3, 2d18h02m
```

| | |
|---|---|
| **B** | BGP. The routing protocol used. |
| **10.160.0.0/23** | The destination of this route including netmask. |

| | |
|---|---|
| **[20/0]** | 20 indicates and administrative distance of 20 out of a range of 0 to 255.<br><br>0 is an additional metric associated with this route, such as in OSPF |
| **10.142.0.74** | The gateway, or next hop. |
| **port3** | The interface used by this route. |
| **2d18h02m** | How old this route is, in this case almost three days old. |

## Perform a sniffer trace

When troubleshooting network traffic, it helps to look inside the headers of packets to determine if they are traveling along the route you expect. Packet sniffing can also be called a network tap, packet capture, or logic analyzing.

If your Carrier-enabled FortiGate unit has NP interfaces that are offloading traffic, this will change the sniffer trace. Before performing a trace on any NP interfaces, disable offloading on those interfaces.

### What can sniffing packets tell you

If you are running a constant traffic application such as ping, packet sniffing can tell you if the traffic is reaching the destination, what the port of entry is on the Carrier-enabled FortiGate unit, if the ARP resolution is correct, and if the traffic is being sent back to the source as expected.

Sniffing packets can also tell you if the Carrier-enabled FortiGate unit is silently dropping packets for reasons such as RPF (Reverse Path Forwarding), also called Anti Spoofing. This prevents an IP packet from being forwarded if its source IP address either does not belong to a locally attached subnet (local interface), or be a hop on the routing between the FortiOS Carrier and another source (static route, RIP, OSPF, BGP). Note that RPF can be disabled by turning on asymmetric routing in the CLI (`config system setting, set asymmetric enable`), however this will disable stateful inspection on the Carrier-enabled FortiGate unit and consequently cause many features to be turned off.

If you configure virtual IP addresses on your Carrier-enabled FortiGate unit, the unit will use those addresses in preference to the physical IP addresses. If not configured properly, secondary IP addresses can cause a broadcast storm. You will notice the secondary address being preferred when you are sniffing packets because all the traffic will be using the virtual IP addresses. This is due to the ARP update that is sent out when the VIP address is configured.

### How to sniff packets

The general form of the internal FortiOS packet sniffer command is:

```
diag sniffer packet <interface_name> <'filter'> <verbose> <count>
```

To stop the sniffer, type `CTRL+C`.

| | |
|---|---|
| **<interface_name>** | The name of the interface to sniff, such as `port1` or `internal`. This can also be `any` to sniff |

| | |
|---|---|
| | all interfaces. |
| **<filter>** | What to look for in the information the sniffer reads. `none` indicates no filtering, and all packets will be displayed as the other arguments indicate.<br><br>The filter must be inside single quotes (‘). |
| **<verbose>** | The level of verbosity as one of:<br><br>**1 -** print header of packets<br>**2 -** print header and data from IP of packets<br>**3 -** print header and data from Ethernet of packets |
| **<count>** | The number of packets the sniffer reads before stopping. If you don’t put a number here, the sniffer will run forever unit you stop it with `<CTRL C>`. |

For a simple sniffing example, enter the CLI command `diag sniffer packet port1 none 1 3`. This will display the next 3 packets on the port1 interface using no filtering, and using verbose level 1. At this verbosity level you can see the source IP and port, the destination IP and port, action (such as ack), and sequence numbers.

In the output below, port 443 indicates these are HTTPS packets, and 172.20.120.17 is both sending and receiving traffic.

```
Head_Office_620b # diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.545306 172.20.120.17.52989 -> 172.20.120.141.443: psh 3177924955 ack 1854307757

0.545963 172.20.120.141.443 -> 172.20.120.17.52989: psh 1854307757 ack 3177925808

0.562409 172.20.120.17.52988 -> 172.20.120.141.443: psh 4225311614 ack 3314279933
```

## Generate specific packets to test the network

If some packets are being delivered as expected while others are not, or after you believe you have fixed the problem, it is a good idea to generate specific traffic to test your network.

For example if you discover through log messages and packet sniffing that Create PDP Context Request messages are not being delivered between two SGSNs, you can generate those specific messages on your network to confirm they are the problem, and later that you have solved the problem and they are now being delivered as expected.

This step requires a third party traffic generation tool, either hardware or software. This is not be supported by Fortinet.